aws

Guide du développeur

Amazon Simple Email Service

Amazon Simple Email Service: Guide du développeur

Table of Contents

Qu'est-ce qu'Amazon SES ?

Amazon Simple Email Service (SES) est une plateforme de messagerie qui vous offre un moyen simple et économique d'envoyer et de recevoir du courrier électronique en utilisant vos propres adresses et domaines de messagerie.

Par exemple, vous pouvez envoyer des e-mails marketing tels que des offres spéciales, des e-mails transactionnels tels que des confirmations de commande et d'autres types de correspondance, notamment des lettres d'information et des notifications système. Si vous recevez le courrier via Amazon SES, vous pouvez développer des solutions logicielles comme des autorépondeurs d'e-mail, des systèmes de désabonnement d'e-mail et des applications qui génèrent des tickets de service clientèle à partir des e-mails entrants.

Pour plus d'informations et des discussions sur une variété de rubriques liées à Amazon SES, consultez le blog AWS Messaging and Targeting (Messagerie et ciblage).

Avantages

Pour une entreprise, créer une solution de messagerie à grande échelle est bien souvent une tâche complexe et coûteuse. Vous devez faire face aux difficultés que représente ce type d'infrastructure, notamment en termes de gestion du serveur de messagerie, de configuration du réseau et de réputation des adresses IP. Par ailleurs, de nombreuses solutions de messagerie tierces imposent un contrat et des négociations de prix, ainsi que d'importants coûts initiaux. Amazon SES écarte ces obstacles et vous permet de bénéficier d'années d'expérience et de l'infrastructure de messagerie sophistiquée développée par Amazon.com pour sa propre base de clients à grande échelle.

Services connexes

Amazon SES s'intègre parfaitement aux autres AWS produits. Par exemple, vous pouvez :

- Ajouter des fonctionnalités d'envoi d'e-mails à n'importe quelle application.
- Vous pouvez envoyer des e-mails d'Amazon EC2 à l'aide d'un kit SDK AWS, à l'aide de l'interface SMTP Amazon SES ou en appelant directement l'API Amazon SES.
- Utilisez AWS Elastic Beanstalk pour créer une application prenant en charge la messagerie, par exemple un programme qui utilise Amazon SES pour envoyer une lettre d'information aux clients.
- Configurez Amazon Simple Notification Service (Amazon SNS) pour qu'il vous informe que vos e-mails ont fait l'objet d'un retour à l'expéditeur ou d'une réclamation, ou qu'ils ont bien été délivrés

au serveur de messagerie du destinataire. Lorsque vous vous servez d'Amazon SES pour recevoir des e-mails, le contenu de ces e-mails peut être publié dans des rubriques Amazon SNS.

- Utilisez le AWS Management Console pour configurer Easy DKIM, qui est un moyen d'authentifier vos e-mails. Même si vous pouvez utiliser Easy DKIM avec n'importe quel fournisseur DNS, sa configuration est d'autant plus simple lorsque vous gérez votre domaine avec Route 53.
- Contrôlez l'accès utilisateur à votre envoi d'e-mail avec AWS Identity and Access Management (IAM).
- Stockez les e-mails que vous recevez dans Amazon Simple Storage Service (Amazon S3).
- Agissez sur les e-mails reçus en déclenchant des fonctions AWS Lambda.
- Utilisez AWS Key Management Service (AWS KMS) pour chiffrer éventuellement le courrier que vous recevez dans votre compartiment Amazon S3.
- Utiliser AWS CloudTrail pour journaliser les appels d'API Amazon SES que vous effectuez à partir de la console ou de l'API Amazon SES.
- Publiez vos événements d'envoi d'e-mails sur Amazon CloudWatch ou Amazon Data Firehose. Si vous publiez vos événements d'envoi d'e-mails sur Firehose, vous pouvez y accéder dans Amazon Redshift, OpenSearch Amazon Service ou Amazon S3.

Tarification

Avec Amazon SES, vous payez en fonction du volume d'e-mails envoyés et reçus. Pour de plus amples informations, consultez la tarification Amazon SES.

Régions et Amazon SES

Amazon SES est disponible dans plusieurs AWS régions du monde. Dans chaque région, AWS dispose de plusieurs zones de disponibilité. Ces zones de disponibilité sont physiquement isolées mais sont reliées par des connexions réseau privées, à latence faible, à débit élevé et à forte redondance. Ces zones de disponibilité nous permettent de fournir des niveaux très élevés de disponibilité et de redondance, tout en réduisant au minimum la latence.

Pour obtenir la liste complète des régions et des points de terminaison Amazon SES, veuillez consulter Points de terminaison et quotas Amazon Simple Email Service dans le document Références générales AWS. Pour en savoir plus sur le nombre de zones de disponibilité disponibles dans chaque région, consultez Infrastructure mondiale AWS.

Cette section contient des informations que vous devez connaître si vous envisagez d'utiliser Amazon SES dans plusieurs AWS régions. Elle traite des sujets suivants :

- Régions et points de terminaison Amazon SES
- Augmentation des limites d'envoi et suppression d'environnement de test (sandbox)
- Vérification des adresses e-mail et des domaines
- Easy DKIM
- Liste de suppression au niveau du compte
- Notifications de commentaire
- Informations d'identification SMTP
- Autorisation d'envoi
- Domaines MAIL FROM personnalisés
- Réception d'e-mails
- Configuration de registres (MX)

Pour des informations générales sur AWS les régions, consultez la section Points AWS de terminaison de service dans le manuel de référence AWS général.

Régions et points de terminaison Amazon SES

Lorsque vous utilisez Amazon SES pour envoyer des e-mails, vous vous connectez à une URL qui fournit un point de terminaison pour l'API SES ou l'interface SMTP. Le Références générales AWS contient une liste complète des points de terminaison que vous utilisez pour envoyer et recevoir des e-mails via Amazon SES. Pour plus d'informations, consultez la section Points de terminaison et quotas Amazon Simple Notification Service dans le document Références générales AWS.

Lorsque vous envoyez des e-mails via Amazon SES, vous pouvez utiliser les URL des lignes spécifiées avec HTTPS dans la colonne Protocol pour faire des demandes HTTPS à l'API SES. Vous pouvez également utiliser les URL des lignes spécifiées avec SMTP dans la colonne Protocol pour envoyer des e-mails à l'aide de l'interface SMTP.

Si vous avez configuré Amazon SES pour recevoir les e-mails qui sont envoyés à votre domaine, vous pouvez utiliser les URL de point de terminaison SMTP entrant (à savoir, les URL qui commencent par « inbound-smtp. ») lorsque vous configurez les registres de serveur de messagerie (MX) dans les paramètres DNS de votre domaine.

> **Note**
>
> Les URL de point de terminaison SMTP entrant ne sont pas des adresses de serveur IMAP. En d'autres termes, vous ne pouvez pas les utiliser pour recevoir des e-mails à l'aide d'une application comme Outlook. Pour un service fournissant un serveur IMAP pour le courrier électronique entrant, consultez Amazon WorkMail.

Augmentation des limites d'envoi et suppression d'environnement de test (sandbox)

Le statut du sandbox de votre compte peut varier d'une AWS région à l'autre. En d'autres termes, si votre compte a été supprimé de l'environnement de test (sandbox) dans la région USA Ouest (Oregaon), il peut encore figurer dans l'environnement de test (sandbox) de la région USA Est (Virginie du Nord), sauf si vous l'avez supprimé de l'environnement de test (sandbox) dans cette région.

Les limites d'envoi peuvent également être différentes en fonction de la AWS région. Par exemple, si votre compte peut envoyer 10 messages par seconde dans la région Europe (Irlande), vous pouvez être en mesure d'envoyer plus ou moins de messages dans d'autres régions.

Lorsque vous envoyez une demande pour que votre compte soit supprimé de l'environnement de test (sandbox) ou lorsque vous envoyez une demande d'augmentation des quotas d'envoi pour votre compte, veillez à choisir toutes les régions AWS auxquelles votre demande s'applique. Vous pouvez envoyer plusieurs demandes dans une seule demande adressée au Centre de support.

Vérification des adresses e-mail et des domaines

Avant de pouvoir envoyer un e-mail avec Amazon SES, vous devez vérifier que vous êtes propriétaire de l'adresse e-mail ou du domaine à partir duquel vous avez l'intention d'envoyer un e-mail. Le statut de vérification des adresses e-mail et des domaines varie également d'une AWS région à l'autre. Par exemple, si vous vérifiez un domaine dans la région USA Ouest (Oregon), vous ne pouvez pas utiliser ce domaine pour envoyer des e-mails dans la région USA Est (Virginie du Nord) tant que vous n'avez pas terminé à nouveau le processus de vérification pour cette région. Pour en savoir plus sur la vérification des adresses e-mail et des domaines, consultez Identités vérifiées dans Amazon SES.

Easy DKIM

Vous devez effectuer le processus de configuration de la fonction Easy DKIM pour chaque région dans laquelle vous souhaitez utiliser Easy DKIM. En d'autres termes, dans chaque région, vous devez utiliser la console Amazon SES ou l'API Amazon SES pour générer des registres TXT. Ensuite, vous devez ajouter tous les registres TXT à la configuration DNS de votre domaine. Pour en savoir plus sur la configuration d'Easy DKIM, consultez Easy DKIM dans Amazon SES.

Liste de suppression au niveau du compte

La liste de suppression au niveau de votre compte Amazon SES s'applique Compte AWS uniquement à votre compte actuel. Région AWS Vous pouvez ajouter ou supprimer manuellement, individuellement ou en bloc, des adresses de votre liste de suppression au niveau du compte en utilisant l'API v2 ou la console SES. Pour en savoir plus sur l'utilisation de votre la liste de suppression au niveau du compte, consultez Utilisation de la liste de suppression au niveau du compte Amazon SES.

Notifications de commentaire

Il existe deux points importants à noter à propos de la configuration des notifications de commentaire dans plusieurs régions :

- Les paramètres d'identité vérifiée, à savoir si vous recevez un commentaire par e-mail ou via Amazon Simple Notification Service (Amazon SNS), s'appliquent uniquement à la région dans laquelle vous les avez définis. Par exemple, si vous vérifiez user@example.com dans les régions USA Ouest (Oregon) et USA Est (Virginie du Nord), et que vous souhaitez recevoir des e-mails de retour à l'expéditeur via les notifications Amazon SES, vous devez utiliser l'API Amazon SES ou la console Amazon SES pour configurer les notifications de commentaire Amazon SNS pour user@example.com dans les deux régions.
- Les rubriques Amazon SNS que vous utilisez pour l'acheminement des commentaires doivent être dans la même région que celle où vous utilisez Amazon SES.

Informations d'identification SMTP

Les informations d'identification que vous utilisez pour envoyer des e-mails via l'interface SMTP d'Amazon SES sont uniques à chaque AWS région. Si vous utilisez l'interface SMTP Amazon SES pour envoyer des e-mails dans plusieurs régions, vous devez générer un ensemble d'informations d'identification SMTP pour chaque région.

> **Note**
>
> Si vous avez créé vos informations d'identification SMTP avant le 10 janvier 2019, elles ont été créées à l'aide d'une ancienne version de la AWS signature. Pour des raisons de sécurité, vous devez supprimer les informations d'identification que vous avez créées avant cette date et les remplacer par de nouvelles informations d'identification. Vous pouvez supprimer d'anciennes informations d'identification à l'aide de la console IAM.

Domaines MAIL FROM personnalisés

Vous pouvez utiliser le même domaine MAIL FROM personnalisé pour les identités vérifiées de différentes régions AWS . Si c'est ce que vous souhaitez faire, vous ne devez publier qu'un seul registre MX sur le serveur DNS du domaine MAIL FROM. Dans ce cas, les notifications de retour à l'expéditeur sont envoyées au point de terminaison des commentaires Amazon SES dans la région que vous avez spécifiée en premier dans le registre MX. Ensuite, Amazon SES redirige les retours à l'expéditeur vers l'identité vérifiée de la région qui a envoyé l'e-mail.

Utilisez les paramètres de registre MX fournis par Amazon SES pendant le processus de configuration MAIL FROM personnalisée pour une identité de l'une des régions. La procédure de configuration MAIL FROM personnalisée est décrite dans Utilisation d'un domaine MAIL FROM personnalisé. À titre de référence, vous pouvez trouver les points de terminaison des commentaires de toutes les régions dans le tableau suivant.

Nom de la région	Points de terminaison de commentaire pour les configurations d'envoi MAIL FROM personnal isées
USA Est (Ohio)	feedback-smtp.us-east-2.amazonses.com
USA Est (Virginie du Nord)	feedback-smtp.us-east-1.amazonses.com
USA Ouest (Californie du Nord)	feedback-smtp.us-west-1.amazonses.com
USA Ouest (Oregon)	feedback-smtp.us-west-2.amazonses.com
Afrique (Le Cap)	feedback-smtp.af-south-1.amazonses.com
Asie-Pacifique (Jakarta)	feedback-smtp.ap-southeast-3.amazonses.com

Nom de la région	Points de terminaison de commentaire pour les configurations d'envoi MAIL FROM personnal isées
Asie-Pacifique (Mumbai)	feedback-smtp.ap-south-1.amazonses.com
Asie-Pacifique (Osaka)	feedback-smtp.ap-northeast-3.amazonses.com
Asie-Pacifique (Séoul)	feedback-smtp.ap-northeast-2.amazonses.com
Asie-Pacifique (Singapour)	feedback-smtp.ap-southeast-1.amazonses.com
Asie-Pacifique (Sydney)	feedback-smtp.ap-southeast-2.amazonses.com
Asie-Pacifique (Tokyo)	feedback-smtp.ap-northeast-1.amazonses.com
Canada (Centre)	feedback-smtp.ca-central-1.amazonses.com
Europe (Francfort)	feedback-smtp.eu-central-1.amazonses.com
Europe (Irlande)	feedback-smtp.eu-west-1.amazonses.com
Europe (Londres)	feedback-smtp.eu-west-2.amazonses.com
Europe (Milan)	feedback-smtp.eu-south-1.amazonses.com
Europe (Paris)	feedback-smtp.eu-west-3.amazonses.com
Europe (Stockholm)	feedback-smtp.eu-north-1.amazonses.com
Israël (Tel Aviv)	feedback-smtp.il-central-1.amazonses.com
Moyen-Orient (Bahreïn)	feedback-smtp.me-south-1.amazonses.com
Amérique du Sud (São Paulo)	feedback-smtp.sa-east-1.amazonses.com
AWS GovCloud (US-Ouest)	feedback smtp. us-gov-west-1.amazonses.com
AWS GovCloud (USA Est)	feedback smtp. us-gov-east-1.amazonses.com

Autorisation d'envoi

Les expéditeurs délégués peuvent uniquement envoyer des e-mails depuis la AWS région où l'identité du titulaire de l'identité est vérifiée. La stratégie d'autorisation d'envoi qui donne l'autorisation à l'expéditeur délégué doit être attachée à l'identité de cette région. Pour en savoir plus sur l'autorisation d'envoi, consultez Utilisation de l'autorisation d'envoi avec Amazon SES.

Réception d'e-mails

À l'exception des compartiments Amazon S3, toutes les AWS ressources que vous utilisez pour recevoir des e-mails avec Amazon SES doivent se trouver dans la même AWS région que le point de terminaison Amazon SES. Par exemple, si vous utilisez Amazon SES dans la région USA Ouest (Oregon), toutes les rubriques Amazon SNS, les clés AWS KMS et les fonctions Lambda que vous utilisez doivent également se trouver dans la région USA Ouest (Oregon). De même, pour recevoir des e-mails avec Amazon SES dans une région, vous devez créer un jeu de règles de réception actif dans cette région.

Le tableau suivant répertorie les points de terminaison de réception d'e-mails pour toutes les AWS régions dans lesquelles Amazon SES prend en charge la réception d'e-mails :

Nom de la région	Région	Point de terminaison de réception d'e-mails
US East (Virginie du Nord)	us-east-1	inbound-smtp.us-east-1.amazonaws.com
USA Est (Ohio)	us-east-2	inbound-smtp.us-east-2.amazonaws.com
USA Ouest (Oregon)	us-west-2	inbound-smtp.us-west-2.amazonaws.com
Asie-Pacifique (Jakarta)	ap-southeast-3	inbound-smtp.ap-southeast-3.amazonaws.com
Asie-Pacifique (Singapour)	ap-southeast-1	inbound-smtp.ap-southeast-1.amazonaws.com

Nom de la région	Région	Point de terminaison de réception d'e-mails
Asie-Pacifique (Sydney)	ap-southeast-2	inbound-smtp.ap-southeast-2.amazonaws.com
Asie-Pacifique (Tokyo)	ap-northeast-1	inbound-smtp.ap-northeast-1.amazonaws.com
Canada (Centre)	ca-central-1	inbound-smtp.ca-central-1.amazonaws.com
Europe (Francfort)	eu-central-1	inbound-smtp.eu-central-1.amazonaws.com
Europe (Irlande)	eu-west-1	inbound-smtp.eu-west-1.amazonaws.com
Europe (Londres)	eu-west-2	inbound-smtp.eu-west-2.amazonaws.com

SES ne prend pas en charge la réception d'e-mails dans les régions suivantes : États-Unis Ouest (Californie du Nord), Afrique (Le Cap), Asie-Pacifique (Mumbai), Asie-Pacifique (Osaka), Asie-Pacifique (Séoul), Europe (Milan), Europe (Paris), Europe (Stockholm), Israël (Tel Aviv), Moyen-Orient (Bahreïn), Amérique du Sud (São Paulo), AWS GovCloud (États-Unis Ouest) et AWS GovCloud (États-Unis Est).

Service Quotas dans Amazon SES

Les sections suivantes répertorient et décrivent les quotas qui s'appliquent aux ressources et aux opérations Amazon SES. Certains quotas peuvent être augmentés, mais pas tous. Pour déterminer si vous pouvez demander une augmentation pour un quota, reportez-vous à la colonne Adjustable (Ajustement).

> **Note**
>
> Les quotas SES correspondent à chacun des quotas Région AWS que vous utilisez dans votre Compte AWS.

Quotas d’envoi d’e-mails

Les quotas suivants s'appliquent à l'envoi d'e-mails via SES.

Quotas d'envoi

Les quotas sont basés sur le nombre de destinataires, plutôt que sur le nombre de messages.

Ressource	Quota par défaut	Ajustable
Nombre d'e-mails pouvant être envoyés par période de 24 heures	Si votre compte est dans l'environnement de test (sandbox), vous pouvez envoyer jusqu'à 200 e-mails par période de 24 heures. Si votre compte est en dehors de l'environnement de test, cette valeur varie en fonction de votre cas d'utilisation.	Oui
Nombre d'e-mails pouvant être envoyés par seconde (taux d'envoi)	Si votre compte est dans l'environnement de test, vous pouvez envoyer 1 e-mail par seconde. Si votre compte est en dehors de l'environnement de test, ce taux varie en fonction de votre cas d'utilisation.	Oui

Quotas de messages

Ressource	Quota par défaut	Ajustable
Utilisation de l'API SES v1 – Taille de message maximale (pièces jointes incluses)	10 Mo par message (après encodage en base64).	Non (Pour les charges de travail dont la taille des messages dépasse 10 Mo, envisagez de migrer vers l'API SES v2.)
Utilisation de l'API SES v2 ou de SMTP – Taille de message maximale (pièces jointes incluses)	40 Mo par message (après encodage en base64).	Non

> **Note**
>
> Les messages de plus de 10 Mo sont soumis à une limitation de la bande passante et, en fonction de votre taux d'envoi, vous risquez d'être réduit à 40 Mo/s. Par exemple, vous pouvez envoyer un message de 40 Mo à raison d'un message par seconde ou de deux messages de 20 Mo par seconde.

Quotas d'expéditeurs et de destinataires

Ressource	Quota par défaut	Ajustable
Nombre maximal de destinataires par message	50 destinataires par message. **Note** Un destinataire correspond à une adresse « To », « CC » ou « BCC ».	Le nombre limite de destinataires n'est pas ajustable . Veuillez contacter votre responsable de AWS compte pour demander cette fonctionnalité après avoir lu la note ci-dessous.

Ressource	Quota par défaut	Ajustable
Nombre maximum d'identités que vous pouvez vérifier	10 000 identités par Région AWS **Note** Une identité est un domaine ou une adresse e-mail que vous utilisez pour envoyer des e-mails via SES.	Veuillez contacter votre gestionnaire de compte AWS pour discuter de votre cas d'utilisation.
Nombre maximum de groupes d'adresses IP dédiées (y compris les groupes d'adresses IP gérées et standard)	50	Non

Note

Avant de demander une augmentation du nombre maximum de destinataires par message, veuillez lire cet article de blog et vous préparer à décrire dans le détail pourquoi votre cas d'utilisation ne peut pas être atteint, en utilisant la limite par défaut de 50 destinataires par message ou en envoyant des messages à des destinataires individuels. La définition de plusieurs destinataires dans la destination d'un message peut entraîner une mauvaise observabilité ainsi qu'une faible délivrabilité et ne doit pas être utilisée, sauf si votre cas d'utilisation l'exige spécifiquement.

Quotas liés à la publication d'événements

Ressource	Quota par défaut	Ajustable
Nombre maximal de jeux de configurations	10 000	Non
Longueur maximale du nom du jeu de configurations	Les noms de jeux de configurations peuvent contenir jusqu'à 64 caractères alphanumériques. Ils peuvent aussi contenir des tirets et des traits de soulignement. Les noms ne peuvent pas contenir des espaces, des caractères accentués ou d'autres caractères spéciaux.	Non
Nombre maximal de destinations d'événements par jeu de configurations	10	Non
Nombre maximum de dimensions par destination de CloudWatch l'événement	10	Non

Quotas de modèle d'e-mail

Ressource	Quota par défaut	Ajustable
Nombre maximum de modèles d'e-mails par e-mail Région AWS	20 000	Non
Taille de modèle maximale	500 Ko	Non

Ressource	Quota par défaut	Ajustable
Nombre maximal de valeurs de remplacement dans chaque modèle	Illimité	N/A
Nombre maximal de destinataires par e-mail basé sur un modèle	50 destinations. Une destination correspond à toute adresse e-mail figurant dans le champ « À », « Cc » ou « Cci ». **Note** Le nombre de destinations que vous pouvez contacter en un seul appel de l'API peut être limité par le taux maximal d'envois de votre compte.	Non

Quotas de réception d'e-mails

Le tableau suivant répertorie les quotas associés à la réception d'e-mails via SES.

Ressource	Quota par défaut	Ajustable
Nombre maximal de règles par ensemble de règles de réception	200	Non
Nombre maximal d'actions par règle de réception	10	Non
Nombre maximal de destinataires par règle de réception	100	Non

Ressource	Quota par défaut	Ajustable
Nombre maximum d'ensembles de règles de réception par Compte AWS	40	Non
Nombre maximum de filtres d'adresses IP par Compte AWS	100	Non
Taille maximale d'e-mail (en-têtes inclus) qui peut être stockée dans un compartiment Amazon S3	40 Mo	Non
Taille maximale d'e-mail (en-têtes inclus) qui peut être publiée à l'aide d'une notification Amazon SNS	150 Ko	Non

Quotas du gestionnaire de courrier

Le tableau suivant répertorie les quotas associés à Mail Manager.

Ressource	Quota par défaut	Ajustable
Nombre maximum de points de terminaison d'entrée ouverts	10	Non
Nombre maximum de points de terminaison d'entrée autorisés	50	Non
Nombre maximal de destinataires par message	100	Non

Ressource	Quota par défaut	Ajustable
Taille maximale des e-mails (y compris les en-têtes)	40 Mo	Non
Nombre maximum de déclarations de politique de trafic	20	Non
Nombre maximum de conditions énoncées dans les déclarations de politique de trafic	10	Non
Nombre maximum de politiques de circulation par région	100	Non
Nombre maximum de relais SMTP	100	Non
Nombre maximum d'ensembles de règles	40	Non
Nombre maximal d'exécutions de règles par message	200	Non
Nombre maximum de conditions par règle	10	Non
Nombre maximal d'actions par règle	10	Non
Nombre maximum d'actions de relais ou d'envoi par ensemble de règles	10	Non
Nombre maximum d'archives actives	10	Non

Ressource	Quota par défaut	Ajustable
Nombre maximum de requêtes de recherche exécutées en parallèle	1	Non
Nombre maximum de demandes d'exportation en cours d'exécution en parallèle	1	Non
Nombre maximal de modifications de conservation pour les archives par semaine	1	Non

Quotas généraux

Le tableau suivant répertorie les quotas qui s'appliquent à la fois à l'envoi et à la réception d'e-mails via SES.

Quotas d'envoi d'API SES

Ressource	Quota par défaut	Ajustable
Fréquence à laquelle vous pouvez appeler les actions d'API Amazon SES	Toutes les actions (à l'exception de `SendEmail`, `SendRawEmail` et `SendTemplatedEmail`) sont limitées à une demande par seconde.	Non
Parties MIME	500	Non

Types d'informations d'identification Amazon SES

Pour interagir avec Amazon Simple Email Service (Amazon SES), vous utilisez des informations d'identification de sécurité pour vérifier votre identité et si vous avez l'autorisation d'interagir avec

Amazon SES. Il existe différents types d'informations d'identification, et celles que vous utilisez dépendent de ce que vous souhaitez effectuer. Par exemple, vous utilisez des clés d'accès AWS lorsque vous envoyez un e-mail à l'aide de l'API Amazon SES, et des informations d'identification SMTP lorsque vous envoyez un e-mail à l'aide de l'interface SMTP Amazon SES.

Le tableau suivant répertorie les types d'informations d'identification que vous pouvez utiliser avec Amazon SES, en fonction de ce que vous faites.

Pour accéder à...	Utilisez ces informations d'identification	De quoi sont composées les informations d'identification	Comment obtenir les informations d'identification
API Amazon SES (Vous pouvez accéder à l'API Amazon SES directement, ou indirectement par le biais d'un kit SDK AWS, de AWS Command Line Interface ou de AWS Tools for Windows PowerShell.)	Clés d'accès AWS	ID de clé d'accès et clé d'accès secrète	Consultez Clés d'accès dans le manuel Références générales AWS. **Note** La bonne pratique en matière de sécurité consiste à utiliser des clés d'accès d'utilisateur AWS Identity and Access Management (IAM) au lieu des clés d'accès Compte AWS. Vos informations d'identification Compte AWS donnent un accès complet à toutes vos ressources AWS. Vous devez donc stocker ces dernières dans un endroit sûr et utiliser les informati

Pour accéder à...	Utilisez ces informations d'identification	De quoi sont composées les informations d'identification	Comment obtenir les informations d'identification
			ons d'identification d'utilisateur IAM pour les interactions quotidiennes avec AWS. Pour de plus amples informations, consultez Informations d'identification du compte racine et informations d'identification de l'utilisateur IAM dans le manuel Références générales AWS.

Pour accéder à...	Utilisez ces informations d'identification	De quoi sont composées les informations d'identification	Comment obtenir les informations d'identification
Interface SMTP Amazon SES	Informations d'identification SMTP	Nom d'utilisateur et mot de passe	Consultez Obtention des informations d'identification SMTP Amazon SES. **Note** Bien que vos informations d'identification SMTP Amazon SES soient différentes de vos clés d'accès AWS et de vos clés d'accès d'utilisateur IAM, les informations d'identification SMTP Amazon SES constituent en fait un type d'informations d'identification. Un utilisateur IAM peut créer des informations d'identification SMTP Amazon SES, mais le propriétaire du compte racine doit s'assurer que la stratégie de l'utilisateur IAM donne à ces informations d'identification SMTP l'autorisation d'accéder aux actions IAM suivantes : « iam:ListU

Pour accéder à...	Utilisez ces informations d'identification	De quoi sont composées les informations d'identification	Comment obtenir les informations d'identification
			sers », « iam:CreateUser », « iam:CreateAccessKey » et « iam:PutUserPolicy ».

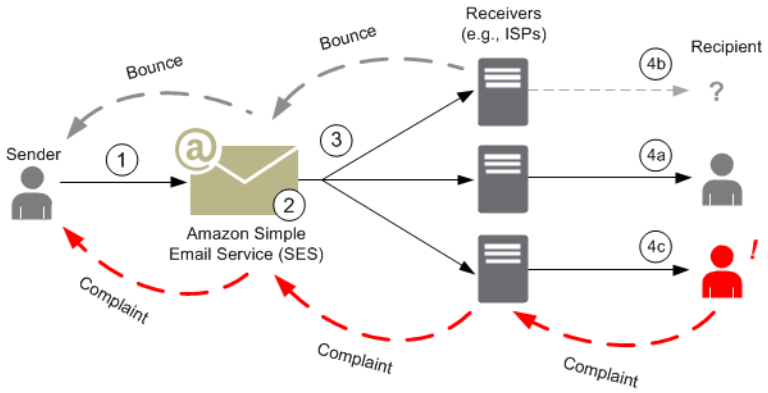
Pour accéder à...	Utilisez ces informations d'identification	De quoi sont composées les informations d'identification	Comment obtenir les informations d'identification
Console Amazon SES	Nom d'utilisateur et mot de passe IAM OU Adresse e-mail et mot de passe	Nom d'utilisateur et mot de passe IAM OU Adresse e-mail et mot de passe	Consultez Nom d'utilisateur et mot de passe IAM et Adresse e-mail et mot de passe dans le manuel Références générales AWS. **Note** La bonne pratique en matière de sécurité consiste à utiliser un nom d'utilisateur et un mot de passe IAM au lieu d'une adresse e-mail et d'un mot de passe. La combinaison de l'adresse e-mail et du mot de passe est destinée à votreCompte AWS. Vous devez donc la stocker dans un endroit sûr et ne pas l'utiliser pour les interactions quotidiennes avec AWS. Pour de plus amples informations, consultez Informations d'identification du compte racine et informations d'identification de l'utilisateur

Pour accéder à...	Utilisez ces informations d'identification	De quoi sont composées les informations d'identification	Comment obtenir les informations d'identification
			IAM dans le manuel Références générales AWS.

Pour en savoir plus sur les différents types d'informations d'identification de sécurité AWS (à l'exception des informations d'identification SMTP qui sont utilisées uniquement pour Amazon SES), consultez Informations d'identification de sécurité AWS dans le document Références générales AWS.

Fonctionnement de l'envoi d'e-mails dans Amazon SES

Cette rubrique décrit ce qui se produit lorsque vous envoyez un e-mail avec SES, ainsi que les divers résultats consécutifs à l'envoi de l'e-mail. L'illustration suivante constitue une présentation générale du processus d'envoi :



1. Une application cliente, agissant en tant qu'expéditeur d'e-mail, formule une requête auprès de SES pour envoyer un e-mail à un ou plusieurs destinataires.
2. Si la demande est valide, SES accepte l'e-mail.
3. SES envoie le message via Internet au destinataire. Une fois que le message est transmis à SES, il est généralement immédiatement envoyé, lors de la première tentative de livraison qui survient normalement dans un délai de quelques millisecondes.

4. À ce stade, il existe différentes possibilités. Par exemple :

    a. Le FAI livre avec succès le message dans la boîte de réception du destinataire.

    b. L'adresse e-mail du destinataire n'existe pas : le FAI envoie une notification de retour à l'expéditeur à SES. SES transmet alors la notification à l'expéditeur.

    c. Le destinataire reçoit le message, mais le juge comme étant du courrier indésirable et enregistre une réclamation auprès de l'ISP. Le FAI, qui dispose d'une boucle de rétroaction configurée avec SES, envoie la réclamation à SES, qui la transmet à l'expéditeur.

Les sections suivantes passent en revue les résultats possibles après l'envoi d'une demande d'e-mail à SES par un expéditeur, et après l'envoi d'un e-mail au destinataire par SES.

Après l'envoi d'une demande d'e-mail à SES par un expéditeur

Lorsque l'expéditeur formule une demande d'envoi d'e-mail à SES, l'appel peut aboutir ou échouer. Les sections suivantes décrivent ce qui se produit dans chaque cas.

La demande d'envoi aboutit

Si la demande faite à SES aboutit, SES renvoie une réponse de réussite à l'expéditeur. Ce message inclut l'ID de message, chaîne de caractères qui identifie de façon unique la demande. Vous pouvez utiliser l'ID de message pour identifier l'e-mail envoyé ou suivre les problèmes rencontrés pendant l'envoi (vous devez stocker votre propre mappage entre un identifiant et l'ID de message SES qui vous est transmis en retour au moment où SES accepte l'e-mail). SES assemble ensuite un message électronique basé sur les paramètres de la demande, analyse le message à la recherche de virus et de contenu douteux, puis l'envoie via Internet à l'aide du protocole SMTP. Votre message est généralement envoyé immédiatement ; la première tentative de livraison s'effectue généralement dans un délai de quelques millisecondes.

> **Note**
>
> Si SES accepte la demande de l'expéditeur et détermine ensuite que le message contient un virus, SES s'arrête de traiter le message et ne tente pas de le remettre au serveur de messagerie du destinataire.

La demande d'envoi échoue

Si la demande d'envoi d'e-mails de l'expéditeur à SES échoue, SES répond à l'expéditeur avec une erreur et supprime l'e-mail. La demande peut échouer pour plusieurs raisons. Par exemple, la demande est peut-être mal formatée ou l'adresse e-mail peut ne pas avoir été vérifiée par l'expéditeur.

La méthode qui permet de déterminer si la demande a échoué dépend de la façon dont vous appelez SES. Voici des exemples de la manière dont les erreurs et les exceptions sont renvoyées :

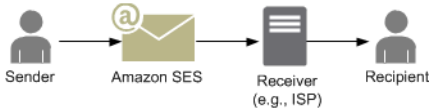
- Si vous appelez SES via l'API de requête (HTTPS) (`SendEmail` ou `SendRawEmail`), les actions renvoient une erreur. Pour plus d'informations, veuillez consulter la Référence d'API Amazon Simple Email Service.
- Si vous utilisez un kit SDK AWS pour un langage de programmation qui utilise des exceptions, l'appel à SES générera une exception MessageRejectedException. (Le nom de l'exception peut varier légèrement selon le kit SDK.)
- Si vous utilisez l'interface SMTP, l'expéditeur reçoit un code de réponse SMTP, mais la manière dont l'erreur est acheminée dépend du client de l'expéditeur. Certains clients peuvent afficher un code d'erreur, mais d'autres peuvent ne pas le faire.

Pour plus d'informations sur les erreurs qui peuvent se produire lorsque vous envoyez un e-mail avec SES, consultez Erreurs d'envoi d'e-mails Amazon SES.

Après l'envoi d'un e-mail par Amazon SES

Si la demande de l'expéditeur à SES aboutit, SES envoie l'e-mail et l'un des résultats suivants se produit :

- La livraison aboutit et le destinataire ne fait pas opposition à l'e-mail – L'e-mail est accepté par le FAI, qui le livre au destinataire. L'illustration suivante présente une livraison ayant abouti.

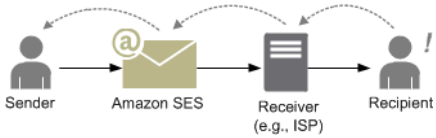


- Message d'erreur définitif – L'e-mail est rejeté par le FAI en raison d'une condition persistante ou par SES car l'adresse e-mail figure sur la liste de suppression SES. Une adresse e-mail figure sur la liste de suppression SES si elle a récemment provoqué un message d'erreur définitif pour un client SES. Un message d'erreur définitif avec un ISP peut se produire lorsque l'adresse du destinataire n'est pas valide. Une notification de message d'erreur définitif est renvoyée par le FAI

à SES, qui informe l'expéditeur par e-mail ou par le biais d'Amazon Simple Notification Service (Amazon SNS), en fonction de la configuration de l'expéditeur. SES informe l'expéditeur des retours de la liste de suppression de la même manière. Le chemin d'un message d'erreur définitif en provenance d'un ISP est présenté dans la figure suivante.

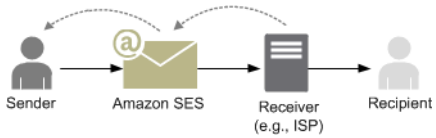
- Message d'erreur temporaire – Le FAI ne peut pas remettre l'e-mail au destinataire en raison d'une condition temporaire, par exemple s'il est trop occupé pour traiter la demande ou si la boîte aux lettres du destinataire est pleine. Un message d'erreur temporaire peut également se produire si le domaine n'existe pas. Le FAI renvoie une notification de message d'erreur temporaire à SES, ou, dans le cas d'un domaine qui n'existe pas, SES ne trouve pas de serveur de messagerie pour le domaine. Dans les deux cas, SES tente à nouveau de livrer l'e-mail pendant une période de temps prolongée. Si SES ne parvient pas à livrer l'e-mail au cours de cette période, il vous envoie une notification de retour à l'expéditeur par e-mail ou via Amazon SNS. Si SES peut remettre l'e-mail au destinataire lors d'une nouvelle tentative, la livraison est réussie. Un message d'erreur temporaire est présenté dans l'illustration suivante. Dans ce cas, SES tente à plusieurs reprises d'envoyer l'e-mail et le FAI est finalement en mesure de le remettre au destinataire.

- Réclamation – L'e-mail est accepté par le FAI et remis au destinataire, mais ce dernier considère l'e-mail comme étant du courrier indésirable et clique sur le bouton « Marquer comme courrier indésirable » dans son client de messagerie. Si SES dispose d'une boucle de rétroaction configurée avec le FAI, une notification de réclamation est envoyée à SES, qui la transmet à l'expéditeur. La plupart des FAI ne fournissent pas l'adresse e-mail du destinataire à l'origine de la réclamation : la notification de réclamation envoyée par SES fournit donc à l'expéditeur une liste de destinataires susceptibles d'avoir envoyé la réclamation, basée sur les destinataires du message d'origine et le FAI à partir duquel SES a reçu la réclamation. Le chemin de la réclamation est présenté dans la figure suivante.



- Réponse automatique – L'e-mail est accepté par le FAI et celui-ci le remet au destinataire. Le FAI envoie ensuite une réponse automatique telle qu'un message d'absence du bureau à SES.

SES transmet la notification de réponse automatique à l'expéditeur. Une réponse automatique est présentée dans l'illustration suivante.



Assurez-vous que votre programme compatible avec SES ne procède pas à plusieurs tentatives d'envoi pour les messages qui génèrent une réponse automatique.

> **Tip**
>
> Vous pouvez utiliser le simulateur de boîte aux lettres (mailbox) SES pour tester une remise réussie, un retour à l'expéditeur, une réclamation, un message d'absence du bureau, ou ce qui se produit lorsqu'une adresse est sur la liste de suppression. Pour de plus amples informations, veuillez consulter Utilisation manuelle du simulateur de boîte aux lettres.

Format d'e-mail dans Amazon SES

Lorsqu'un client envoie une requête à Amazon SES, Amazon SES génère un message électronique conforme à la spécification Format de message Internet (RFC 5322). Un e-mail se compose d'un en-tête, d'un corpset d'une enveloppe, comme décrit ci-dessous.

- En-tête – Contient des instructions de routage et des informations sur le message. Il peut s'agir, par exemple, de l'adresse de l'expéditeur, l'adresse du destinataire, l'objet et la date. L'en-tête est analogue aux informations de la partie supérieure d'une lettre postal, même si elle peut contenir de nombreux autres types d'informations, comme le format du message.
- Corps – Contient le texte du message lui-même.
- Enveloppe – Contient les informations de routage communiquées entre le client de messagerie et le serveur de messagerie au cours de la session SMTP. Ces informations de l'enveloppe de l'e-mail sont analogues à celles figurant sur une enveloppe postale. Les informations de routage de l'enveloppe de l'e-mail sont généralement identiques aux informations de routage dans l'en-tête de l'e-mail, mais pas toujours. Par exemple, lorsque vous envoyez une copie carbone invisible (Cci), l'adresse du destinataire réel (dérivée de l'enveloppe) n'est pas la même que l'adresse du destinataire « À » qui est affiché sur le client de messagerie du destinataire, dérivée de l'en-tête.

Voici un exemple simple d'e-mail. L'en-tête est suivie d'une ligne vide, puis du corps de l'e-mail. L'enveloppe n'est pas affichée, car elle est échangée entre le client et le serveur de messagerie au cours de la session SMTP, et ne fait pas partie de l'e-mail lui-même.

```
Received: from abc.smtp-out.amazonses.com (123.45.67.89) by in.example.com
 (87.65.43.210); Fri, 17 Dec 2010 14:26:22
From: "Andrew" <andrew@example.com>;
To: "Bob" <bob@example.com>
Date: Fri, 17 Dec 2010 14:26:21 -0800
Subject: Hello
Message-ID: <61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>
Accept-Language: en-US
Content-Language: en-US
Content-Type: text/plain; charset="us-ascii"
Content-Transfer-Encoding: quoted-printable
MIME-Version: 1.0

Hello, I hope you are having a good day.

-Andrew
```

Les sections suivantes présentent les en-têtes et les corps d'e-mail, et identifient les informations que vous devez fournir lorsque vous utilisez Amazon SES.

En-tête d'e-mail

Il y a un en-tête par message électronique. Chaque ligne de l'en-tête contient un champ suivie d'un signe deux points et d'un corps de champ. Lorsque vous lisez un e-mail dans un client de messagerie, celui-ci affiche généralement les valeurs des champs d'en-tête suivants :

- To – Adresses e-mail des destinataires du message.
- CC – Adresses e-mail des destinataires en copie carbone du message.
- From – Adresse e-mail à partir de laquelle l'e-mail est envoyé.
- Subject – Résumé du sujet du message.
- Date – Heure et date auxquelles l'e-mail est envoyé.

Il existe de nombreux autres champs d'en-tête qui fournissent des informations de routage et décrivent le contenu du message. Les clients de messagerie ne montrent généralement pas

ces champs à l'utilisateur. Pour obtenir la liste complète des champs d'en-tête acceptés par Amazon SES, consultez Champs d'en-tête Amazon SES. Lorsque vous utilisez Amazon SES, vous devez plus particulièrement comprendre la différence entre les champs d'en-tête « From », « Reply-To » et « Return-Path (Chemin de retour) ». Comme indiqué précédemment, l'adresse « From » est l'adresse e-mail de l'expéditeur du message, tandis que « Reply-To » et « Return-Path (Chemin de retour) » sont respectivement définis comme suit :

- Reply-To – Adresse e-mail à laquelle les réponses seront envoyées. Par défaut, les réponses sont envoyées à l'adresse e-mail de l'expéditeur d'origine.
- Return-Path (Chemin de retour) – Adresse e-mail à laquelle les retours à l'expéditeur et les réclamations de messages doivent être envoyés. « Return-Path (Chemin de retour) » est parfois appelé « envelope from », « envelope sender » ou « MAIL FROM ».

> **Note**
>
> Lorsque vous utilisez Amazon SES, nous vous recommandons de toujours définir le paramètre « Return-Path (Chemin de retour) » afin d'être informé des retours à l'expéditeur et de prendre des mesures correctives si nécessaire.

Pour établir la correspondance entre un message retourné à l'expéditeur et le destinataire visé, vous pouvez utiliser la méthode de l'adresse de retour variable (VERP). Avec VERP, vous définissez un « Return-Path (Chemin de retour) » distinct pour chaque destinataire ; si le message est retourné, vous savez automatiquement de quel destinataire provient le retour, plutôt que de devoir ouvrir le message de retour à l'expéditeur et l'analyser.

Corps d'e-mail

Le corps d'un e-mail contient le texte du message. Le corps peuvent être envoyé dans les formats suivants :

- HTML – Si le client de messagerie du destinataire peut interpréter le format HTML, le corps peut inclure du texte formaté et des hyperliens
- Texte brut – Si le client de messagerie du destinataire est basé sur du texte, le corps ne doit contenir aucun caractère non imprimable.
- HTML et texte brut – Lorsque vous utilisez les deux formats pour envoyer le même contenu dans un message unique, le client de messagerie du destinataire choisit le format à afficher, en fonction des ses capacités.

Si vous envoyez un message électronique à un grand nombre de destinataires, il est logique d'utilisez les deux formats HTML et texte. Les destinataires disposant de clients de messagerie compatibles avec le format HTML pourront cliquer sur les hyperliens intégrés dans le message. Pour les destinataires utilisant des clients de messagerie basés sur le texte, vous devrez inclure des URL qu'ils pourront copier et ouvrir à l'aide d'un navigateur Web.

Informations de l'e-mail que vous devez fournir à Amazon SES

Lorsque vous envoyez un e-mail avec Amazon SES, les informations de l'e-mail que vous devez fournir dépendent de la façon dont vous appelez Amazon SES. Vous pouvez fournir une quantité minimum d'informations et laisser Amazon SES gérer la mise en forme pour vous. Ou, si vous souhaitez effectuer une opération plus avancée comme envoyer une pièce jointe, vous pouvez fournir le message brut vous-même. Les sections suivantes décrivent ce que vous devez fournir lorsque vous envoyez un e-mail à l'aide de l'API Amazon SES, de l'interface SMTP Amazon SES ou de la console Amazon SES.

API Amazon SES

Si vous appelez l'API Amazon SES directement, vous appelez l'API `SendEmail` ou `SendRawEmail`. La quantité d'informations que vous devez fournir dépend de l'API que vous appelez.

- L'API `SendEmail API` vous demande de ne fournir qu'une adresse source, une adresse de destination, un objet de message et un corps de message. Vous pouvez, si vous le souhaitez, fournir des adresses « Reply-To ». Lorsque vous appelez cette API, Amazon SES assemble automatiquement un message Multipurpose Internet Mail Extensions (MIME) en plusieurs parties correctement formaté et optimisé pour être affiché dans un logiciel client de messagerie. Pour plus d'informations, consultez Envoi d'e-mails formatés à l'aide de l'API Amazon SES.
- L'API `SendRawEmail` fournit à l'utilisateur avancé la flexibilité de mettre en forme et envoyer son propre message électronique brut en indiquant les en-têtes, les parties MIME et les types de contenu. `SendRawEmail` est généralement utilisé par les utilisateurs avancés. Vous devez fournir le corps du message et tous les champs d'en-tête indiqués comme requis dans la spécification Format de message Internet (RFC 5322). Pour plus d'informations, consultez Envoi d'e-mails bruts à l'aide de l'API Amazon SES v2.

Si vous utilisez un kit SDK AWS pour appeler l'API Amazon SES, vous fournissez les informations ci-dessus aux fonctions correspondantes (par exemple, `SendEmail` et `SendRawEmail` pour Java).

Pour en savoir plus sur l'utilisation de l'API Amazon SES pour l'envoi d'e-mails, consultez Utilisation de l'API Amazon SES pour envoyer un e-mail.

Interface SMTP Amazon SES

Lorsque vous accédez à Amazon SES via l'interface SMTP, votre application cliente SMTP assemble le message de façon à ce que les informations à fournir dépendent de l'application que vous utilisez. Au minimum, l'échange SMTP entre un client et un serveur requiert une adresse source, une adresse de destination et des données de message.

Pour en savoir plus sur l'utilisation de l'interface SMTP Amazon SES pour l'envoi d'e-mails, consultez Utilisation de l'interface SMTP d'Amazon SES pour envoyer des e-mails.

Console Amazon SES

Lorsque vous envoyez un e-mail à l'aide de la console Amazon SES, la quantité d'informations que vous devez fournir varie selon que vous choisissez d'envoyer un e-mail formaté ou un e-mail brut.

- Pour envoyer un e-mail formaté, vous devez fournir une adresse source, une adresse de destination, un objet de message et un corps de message. Amazon SES assemble automatiquement un message électronique MIME en plusieurs parties correctement formaté et optimisé pour être affiché dans un logiciel client de messagerie. Vous pouvez également spécifier un champ « Reply-To » et « Return-Path (Chemin de retour) ».
- Pour envoyer un e-mail brut, vous fournissez l'adresse source, une adresse de destination et le contenu du message, qui doit contenir le corps du message et tous les champs d'en-tête indiqués comme requis dans la spécification Format de message Internet (RFC 5322).

Présentation de la délivrabilité des e-mails dans Amazon SES

Vous souhaitez que vos destinataires lisent vos e-mails, les trouvent intéressants et ne les signalent pas comme étant du courrier indésirable. En d'autres termes, vous souhaitez maximiser la délivrabilité des e-mails, c'est-à-dire le pourcentage d'e-mails qui arrive dans la boîte de réception de vos destinataires. Cette rubrique décrit les concepts de délivrabilité d'e-mails que vous devez maîtriser lorsque vous utilisez Amazon SES.

Pour optimiser la délivrabilité, vous devez comprendre les problèmes liés à la livraison d'e-mails et adopter des mesures proactives pour les prévenir, rester informés de l'état des e-mails que vous envoyez, mais également améliorer votre programme d'envoi d'e-mails, si nécessaire, afin

d'augmenter les possibilités de messages délivrés. Les sections suivantes présentent les concepts associés à ces étapes et la manière dont Amazon SES vous aide tout au long du processus.

Comprendre les problèmes liés à la livraison d'e-mails

Dans la plupart des cas, vos messages sont livrés avec succès aux destinataires qui les attendent. Toutefois, dans certains cas, une livraison peut échouer ou un destinataire peut souhaiter ne pas recevoir les e-mails que vous envoyez. Les retours à l'expéditeur, les réclamations et les listes de suppression, liés à ces problèmes de livraison, sont décrits dans les sections suivantes.

Retour à l'expéditeur

Si un récepteur (par exemple, un fournisseur de messagerie) ne parvient pas à remettre un message à votre destinataire, il le retourne à Amazon SES. Amazon SES vous informe de ce retour par e-mail ou par le biais d'Amazon Simple Notification Service (Amazon SNS), en fonction de la manière dont vous avez configuré votre système. Pour plus d'informations, consultez Configuration de notifications d'événement pour Amazon SES.

Il y a des messages d'erreur définitifs et des messages d'erreur temporaires, comme suit :

- Message d'erreur définitif – Échec définitif de livraison d' e-mail. Par exemple, la boîte de réception n'existe pas. Amazon SES ne fait pas de nouvelle tentative de livraison, à l'exception des échecs de recherche DNS. Nous vous recommandons vivement de ne pas répéter les tentatives d'envoi vers des adresses e-mail qui renvoient des messages d'erreur définitifs.
- Message d'erreur temporaire – Échec temporaire de livraison d'e-mail. Par exemple, la boîte de réception est pleine, le nombre de connexions est trop important (également appelé limitation), ou la connexion arrive à expiration. Amazon SES effectue plusieurs tentatives en cas de message d'erreur temporaire. Si Amazon SES ne parvient toujours pas à remettre l'e-mail, il cesse d'essayer.

Amazon SES vous informe des messages d'erreur définitifs et des messages d'erreur temporaires qui ne feront plus l'objet de nouvelles tentatives. Toutefois, seuls les messages d'erreur définitifs sont comptabilisés dans votre taux de retours à l'expéditeur et dans les métriques de retours à l'expéditeur que vous récupérez à l'aide de la console Amazon SES ou de l'API `GetSendStatistics`.

Les retours à l'expéditeur peuvent également être synchrones ou asynchrones. Un retour à l'expéditeur synchrone se produit lorsque les serveurs de messagerie de l'expéditeur et du destinataire communiquent activement. Un retour à l'expéditeur asynchrone se produit lorsqu'un récepteur accepte initialement un message électronique, mais qu'il ne parvient pas ensuite à le remettre au destinataire.

Plainte

La plupart des programmes clients de messagerie fournissent un bouton intitulé « Marquer comme courrier indésirable », ou similaire, qui permet de déplacer le message vers un dossier de courrier indésirable et de le transmettre au fournisseur de messagerie. De plus, la plupart des fournisseurs de messagerie gèrent une adresse « abuse » (par exemple, abuse@example.net), où les utilisateurs peuvent transférer les messages indésirables et demander au fournisseur de messagerie de prendre des mesures préventives. Dans les deux cas, le destinataire formule une réclamation.
Si le fournisseur de messagerie conclut que vous êtes un expéditeur de courrier indésirable et qu'Amazon SES a une boucle de rétroaction est configurée avec le fournisseur de messagerie, celui-ci enverra la réclamation à Amazon SES. Lorsqu'Amazon SES reçoit une réclamation de ce type, il vous la transfère par e-mail ou via une notification Amazon SNS, en fonction de la manière dont vous avez configuré votre système. Pour plus d'informations, consultez Configuration de notifications d'événement pour Amazon SES. Nous vous recommandons de ne pas répéter les tentatives d'envoi vers des adresses e-mail qui génèrent des réclamations.

Liste de suppression globale

La liste de suppression globale Amazon SES, possédée et gérée par SES pour protéger la réputation des adresses dans le pool d'adresses IP partagées de SES, contient les adresses e-mail de destinataires qui ont récemment provoqué un message d'erreur répétitif pour un client SES. Si vous essayez d'envoyer un e-mail via SES à une adresse figurant dans la liste de suppression, l'appel à SES aboutit, mais SES traite l'e-mail comme un message d'erreur définitif au lieu d'essayer de l'envoyer. Comme tout message d'erreur définitif, les retours de la liste de suppression sont comptabilisés dans votre quota d'envoi et votre taux de retours. Les adresses e-mail peuvent rester dans la liste de suppression pendant 14 jours maximum. Si vous êtes sûr que l'adresse e-mail à laquelle vous tentez d'envoyer est valide, vous pouvez ignorer la liste de suppression globale en vous assurant que l'adresse n'est pas répertoriée dans la liste de suppression au niveau de votre compte et SES tentera toujours de remettre le message. Mais s'il y a rebond, cela affectera votre propre réputation, mais les autres expéditeurs n'auront pas de rebond, car car ils ne peuvent pas envoyer à cette adresse e-mail s'ils n'utilisent pas leur propre liste de suppression au niveau du compte. Pour mieux comprendre la liste de suppression des e-mails au niveau du compte, voir Utilisation de la liste de suppression au niveau du compte Amazon SES.

Soyez proactif

L'envoi de courrier indésirable en nombre, ou spam, constitue un des principaux problèmes liés aux e-mails sur Internet (courrier indésirable). Les fournisseurs de messagerie prennent de nombreuses mesures pour éviter que leurs clients ne reçoivent du courrier indésirable. Amazon SES prend également des mesures pour diminuer la probabilité que les fournisseurs de messagerie considèrent vos e-mails comme étant du courrier indésirable. Amazon SES utilise la vérification, l'authentification, les quotas d'envoi et le filtrage de contenu. Amazon SES gère également une réputation de confiance avec les fournisseurs de messagerie et requiert de votre part l'envoi d'e-mails de haute qualité. Amazon SES effectue automatiquement quelques opérations pour vous (par exemple, le filtrage de contenu) ; dans d'autres cas, il fournit les outils (tels que l'authentification), ou vous guide dans la bonne direction (quotas d'envoi). Les sections suivantes présentent des informations supplémentaires sur chaque concept.

Vérification

Malheureusement, il est possible pour un spammeur de falsifier l'en-tête d'un e-mail et d'usurper l'adresse e-mail d'origine pour faire comme si l'e-mail provenait d'une source différente. Pour maintenir la confiance entre Amazon SES et les fournisseurs de messagerie, Amazon SES doit s'assurer que ses expéditeurs sont les personnes qu'ils déclarent être. Vous êtes donc tenu de vérifier toutes les adresses e-mail à partir desquelles vous envoyez des e-mails à l'aide

d'Amazon SES pour protéger votre identité d'envoi. Vous pouvez vérifier les adresses e-mail à l'aide de la console Amazon SES ou de l'API Amazon SES. Vous pouvez également vérifier des domaines complets. Pour plus d'informations, consultez Création d'une identité d'adresse e-mail et Création d'une identité de domaine.

Si votre compte est toujours dans l'environnement de test Amazon SES, vous devez également vérifier toutes les adresses des destinataires, à l'exception de celles fournies par le simulateur de boîte aux lettres (mailbox) Amazon SES. Pour en savoir plus sur la sortie de l'environnement de test, consultez Demande d'accès à la production (sortie du sandbox d'Amazon SES). Pour en savoir plus sur le simulateur de boîte aux lettres email (mailbox), consultez Utilisation manuelle du simulateur de boîte aux lettres.

Authentification

L'authentification est un autre moyen qui vous permet de vous identifier auprès des fournisseurs de messagerie. Lorsque vous authentifiez un e-mail, vous apportez la preuve que vous êtes le propriétaire du compte et que vos e-mails n'ont pas été modifiés en transit. Dans certains cas, les fournisseurs de messagerie refusent de transférer un e-mail qui n'est pas authentifié. Amazon SES prend en charge deux méthodes d'authentification : SPF (Sender Policy Framework) et DKIM (DomainKeys Identified Mail). Pour plus d'informations, consultez Configuration des identités dans Amazon SES.

Quotas d'envoi

Si un fournisseurs de messagerie détecte des pics soudains et inattendus dans le volume ou le taux de vos e-mails, il peut vous soupçonner d'être un expéditeur de courrier indésirable et bloquer vos e-mails. Par conséquent, chaque compte Amazon SES dispose d'un ensemble de quotas d'envoi. Ces quotas limitent le nombre d'e-mails que vous pouvez envoyer en 24 heures et le nombre que vous pouvez envoyer par seconde. Ces quotas d'envoi aident à protéger votre crédibilité auprès des fournisseurs de messagerie.

Dans la plupart des cas, si vous êtes un nouvel utilisateur, Amazon SES vous permet d'envoyer une petite quantité d'e-mails chaque jour. Si l'e-mail que vous envoyez est acceptable pour les fournisseurs de messagerie, nous augmentons automatiquement ce quota. Au fil du temps, vos quotas d'envoi augmentent constamment afin que vous puissiez envoyer de plus grandes quantités d'e-mails à des vitesses plus importantes. Vous pouvez également créer une demande d'augmentation des limites d'envoi SES pour demander des augmentations de quota supplémentaires.

Pour en savoir plus sur les quotas d'envoi et sur la manière de les augmenter, consultez Gestion de vos limites d'envoi Amazon SES.

Filtrage de contenu

De nombreux fournisseurs de messagerie utilisent le filtrage de contenu pour déterminer si les e-mails entrants sont indésirables. Les filtres de contenu recherchent du contenu et bloquent l'e-mail si celui-ci a le profil de courrier indésirable. Amazon SES utilise également des filtres de contenu. Lorsque votre application envoie une demande à Amazon SES, Amazon SES assemble un message électronique en votre nom, puis scanne l'en-tête et le corps de ce message afin de déterminer si son contenu peut être considéré comme courrier indésirable par les fournisseurs de service Si vos messages sont considérés comme du courrier indésirable par les filtres de contenu utilisés par Amazon SES, votre réputation auprès d'Amazon SES en sera négativement affectée.

Amazon SES numérise également tous les messages à la recherche de virus. Si un message contient un virus, Amazon SES ne tente pas de remettre le message au serveur de messagerie du destinataire.

Réputation

En matière d'envoi d'e-mails, la réputation est importante, car elle correspond au degré de certitude qu'une adresse IP, une adresse e-mail ou un domaine d'envoi n'est pas la source du courrier indésirable. Amazon SES entretient une solide réputation avec les fournisseurs de messagerie afin que ces derniers remettent vos e-mails dans les boîtes de réception de vos destinataires. De même, vous devez conserver une réputation de confiance avec Amazon SES. Vous créez votre réputation avec Amazon SES en envoyant du contenu de grande qualité. Lorsque vous envoyez du contenu de grande qualité, votre réputation devient plus fiable au fil du temps et Amazon SES augmente vos quotas d'envoi. Les réclamations et retours à l'expéditeur excessifs ont un impact négatif sur votre réputation et peuvent amener Amazon SES à réduire les quotas d'envoi pour votre compte, ou à résilier votre compte Amazon SES.

Afin de vous aider à conserver votre réputation, vous pouvez utiliser le simulateur de boîte aux lettres email (mailbox) lorsque vous testez votre système, au lieu d'envoyer des e-mails à des adresses électroniques que vous avez créées vous-même. Les e-mails envoyés au simulateur de boîte aux lettres email (mailbox) ne sont pas pris en compte dans les métriques de retour à l'expéditeur et de réclamation. Pour en savoir plus sur le simulateur de boîte aux lettres email (mailbox), consultez Utilisation manuelle du simulateur de boîte aux lettres.

E-mail de haute qualité

Un e-mail de haute qualité est un e-mail que les destinataires jugent précieux et souhaitent recevoir. Le mot « précieux » signifie différentes choses selon les destinataires et peut se présenter sous la forme d'offres, de confirmations de commande, de reçus, de lettres d'information, etc. En définitive, votre délivrabilité repose sur la qualité des e-mails que vous envoyez, car les fournisseurs de messagerie bloquent les e-mails qu'ils jugent comme étant de mauvaise qualité.

Restez informé

Que vos livraisons de message échouent, que les destinataires formulent des réclamations au sujet de vos e-mails ou qu'Amazon SES livre un e-mail au serveur de messagerie d'un destinataire, Amazon SES vous aide à identifier les problèmes en vous fournissant des notifications et en vous permettant de surveiller facilement vos statistiques d'utilisation.

Notifications

Lorsqu'un e-mail est retourné à l'expéditeur, le fournisseur de messagerie en informe Amazon SES et Amazon SES vous en informe. Amazon SES vous informe des messages d'erreur définitifs et des messages d'erreur temporaires qui ne feront plus l'objet de nouvelles tentatives. De nombreux fournisseurs de messagerie font également suivre les réclamations, et Amazon SES configure des boucles de rétroaction de réclamations avec les principaux fournisseurs de messagerie afin que vous n'ayez pas à le faire. Amazon SES peut vous informer des retours à l'expéditeur, des réclamations et des messages délivrés de deux manières : vous pouvez configurer votre compte de manière à recevoir des notifications via Amazon SNS ou par e-mail (retours à l'expéditeur et réclamations uniquement). Pour plus d'informations, consultez Configuration de notifications d'événement pour Amazon SES.

Statistiques d'utilisation

Amazon SES fournit des statistiques d'utilisation qui vous permettent de prendre connaissance des livraisons de message ayant échoué, afin de déterminer et de remédier aux causes premières. Vous pouvez afficher vos statistiques d'utilisation à l'aide de la console Amazon SES ou en appelant l'API Amazon SES. Vous pouvez consulter le nombre de message délivrés, de retours à l'expéditeur, de réclamations et d'e-mails infectés par un virus et rejetés ; vous pouvez également visualiser vos quotas d'envoi pour être certain de ne pas les dépasser.

Améliorer votre programme d'envoi d'e-mails

Si vous recevez un grand nombre de retour à l'expéditeur et de réclamations, il est temps de réévaluer votre stratégie d'envoi d'e-mails. N'oubliez pas que les retours à l'expéditeur, les réclamations et les tentatives d'envoi d'e-mails de mauvaise qualité constituent un acte abusif et exposent votre Compte AWS à un risque de résiliation. En fin de compte, vous devez vous assurer d'utiliser Amazon SES pour envoyer des e-mails de haute qualité et ce, uniquement aux destinataires qui souhaitent les recevoir.

Diffusion au moins une fois

Amazon SES stocke des copies de vos messages sur plusieurs serveurs à des fins de redondance et de haute disponibilité. Dans de rares occasions, l'un des serveurs qui stockent la copie d'un message peut être indisponible lors de la réception ou de la suppression d'un message.

Dans ce cas, la copie du message n'est pas supprimée sur le serveur indisponible, et il est possible qu'il soit à nouveau copié lorsque vous recevez des messages. Concevez les applications afin qu'elles soient idempotentes (c.-à-d. qu'elles ne doivent pas être affectées si le même message est traité plus d'une fois).

Bonnes pratiques concernant l'envoi d'e-mails à l'aide d'Amazon SES

La méthode avec laquelle vous gérez les communications par e-mail avec vos clients est appelée programme de messagerie. Plusieurs facteurs peuvent entraîner la réussite ou l'échec de votre programme de messagerie. Ces facteurs peuvent sembler déroutants ou mystérieux de prime abord. Cependant, en comprenant comment les e-mails sont remis et en suivant quelques bonnes pratiques, vous pouvez augmenter les chances que vos e-mails arrivent avec succès dans les boîtes de réception de vos clients.

Rubriques

Métriques de la réussite pour les programmes de messagerie

Il existe plusieurs métriques qui aident à mesurer la réussite de votre programme de messagerie.

Cette section fournit des informations sur les métriques suivantes :

- Réclamations
- Qualité des messages

Retours à l'expéditeur

Un retour à l'expéditeur a lieu lorsqu'un e-mail ne peut pas être remis au destinataire prévu. Il existe deux types de retours à l'expéditeur : ceux entraînant un message d'erreur définitif et ceux entraînant un message d'erreur temporaire. Un message d'erreur définitif a lieu lorsque l'e-mail ne peut pas être remis en raison d'un problème persistant, par exemple, lorsqu'une adresse e-mail n'existe pas. Un message d'erreur temporaire a lieu lorsqu'un problème temporaire empêche la remise d'un e-mail. Cela peut se produire, par exemple, lorsque la boîte de réception d'un destinataire est pleine ou lorsque le serveur de réception est provisoirement indisponible. Amazon SES gère les messages d'erreur temporaires en retentant de remettre les e-mails concernés pendant un certain temps.

Il est essentiel de surveiller le nombre de messages d'erreur définitifs dans votre programme de messagerie et de supprimer les adresses e-mail donnant lieu à ces erreurs de vos listes de destinataires. Lorsque des serveurs de messagerie détectent un taux élevé de messages d'erreur définitifs, ils supposent que vous ne connaissez pas bien vos destinataires. Par conséquent, un taux élevé de messages d'erreur définitifs peut avoir un impact négatif sur la délivrabilité de vos messages.

Les consignes suivantes peuvent vous aider à éviter les retours à l'expéditeur et à améliorer votre réputation d'expéditeur :

- Essayez de maintenir votre taux de messages d'erreur définitifs sous la barre des 5 %. Moins votre programme de messagerie donnera lieu à des messages d'erreur définitifs, plus les FAI considéreront vos messages comme légitimes et utiles. Ce taux doit être considéré comme un objectif réaliste et raisonnable, mais il ne s'agit pas d'une règle universelle pour tous les FAI.
- Ne louez ou n'achetez jamais des listes d'adresses e-mail. Ces listes peuvent contenir un grand nombre d'adresses non valides, ce qui peut augmenter considérablement vos taux de messages d'erreur définitifs. De plus, ces listes peuvent contenir des pièges à courrier indésirable, des adresses e-mail utilisées pour intercepter des expéditeurs illégitimes. Si vos messages arrivent dans un piège à courrier indésirable, cela peut nuire définitivement à votre taux de remise et à votre réputation d'expéditeur.
- Gardez votre liste à jour. Si vous n'avez pas envoyé d'e-mail à des destinataires depuis longtemps, essayez de valider les statuts de vos clients par d'autres moyens (par exemple, l'activité de connexion au site web ou l'historique d'achats).

- Si vous ne disposez pas d'une méthode pour vérifier les statuts de vos clients, envisagez d'envoyer un e-mail de reconquête. Un e-mail de reconquête classique indique que vous n'avez pas eu de nouvelles de votre client depuis longtemps et encourage celui-ci à confirmer qu'il souhaite toujours recevoir vos e-mails. Après avoir envoyé un e-mail de reconquête, purgez toutes les destinataires qui n'ont pas répondu de vos listes.

Lorsque vous recevez des retours à l'expéditeur, il est essentiel de réagir de manière appropriée en respectant les règles suivantes :

- Si une adresse e-mail donne lieu à des messages d'erreur définitifs, supprimez-la immédiatement de votre liste. Ne tentez pas d'envoyer à nouveau des messages à de telles adresses. Lorsque les messages d'erreur définitifs sont répétés, ils s'accumulent et finissent par nuire à votre réputation auprès du FAI du destinataire.
- Assurez-vous que l'adresse que vous utilisez pour recevoir des notifications de retour à l'expéditeur est en mesure de recevoir des e-mails. Pour en savoir plus sur la configuration des notifications de retour à l'expéditeur et de réclamation, consultez Configuration de notifications d'événement pour Amazon SES.
- Si vos e-mails entrants proviennent d'un FAI, et non de vos propres serveurs internes, un flux de notifications de retour à l'expéditeur peut arriver dans votre dossier de courrier indésirable ou être complètement supprimé. Dans l'idéal, vous ne devez pas utiliser une adresse e-mail hébergée pour recevoir des retours à l'expéditeur. Si vous devez néanmoins en utiliser une, vérifiez souvent le dossier de courrier indésirable et ne marquez pas les messages de retour à l'expéditeur comme du courrier indésirable. Dans Amazon SES, vous pouvez spécifier l'adresse à laquelle les notifications de retours à l'expéditeur sont envoyées.
- En règle générale, un retour à l'expéditeur fournit l'adresse de la boîte de réception qui refuse la remise. Toutefois, si vous avez besoin de données plus détaillées pour faire correspondre une adresse de destinataire à une campagne d'e-mail particulière, incluez un en-tête X avec une valeur que vous pouvez suivre dans votre système de suivi interne. Pour de plus amples informations, veuillez consulter Champs d'en-tête Amazon SES.

Réclamations

Une réclamation a lieu lorsqu'un destinataire d'un e-mail clique sur le bouton « Marquer comme courrier indésirable » (ou équivalent) dans son client de messagerie basée sur le web. Si vous accumulez de nombreuses réclamations de ce type, le FAI suppose que vous envoyez du courrier indésirable. Cela a un impact négatif sur votre taux de délivrabilité et votre réputation d'expéditeur.

Certains FAI, mais pas tous, vous informent lorsqu'une réclamation est signalée ; cette opération est appelée boucle de rétroaction. Amazon SES vous fait suivre automatiquement les réclamations à partir des FAI qui vous fournissent des boucles de rétroaction.

Les consignes suivantes peuvent vous aider à éviter les réclamations et à améliorer votre réputation d'expéditeur :

- Essayez de maintenir votre taux de réclamations sous la barre des 0,1 %. Moins votre programme de messagerie donnera lieu à des réclamations, plus les FAI considéreront vos messages comme légitimes et utiles. Ce taux doit être considéré comme un objectif réaliste et raisonnable, mais il ne s'agit pas d'une règle universelle pour tous les FAI.
- Si un client soumet une réclamation à propos d'un e-mail marketing, vous devez immédiatement arrêter d'envoyer des e-mails marketing à ce client. Toutefois, si votre programme de messagerie inclut également d'autres types d'e-mails (comme des e-mails de notification ou transactionnels), il peut être acceptable de continuer à envoyer ces types de messages au destinataire à l'origine de la réclamation.
- Comme avec les messages d'erreur définitifs, si vous disposez d'une liste que vous n'avez pas utilisée pour vos envois depuis un moment, assurez-vous que vos destinataires comprennent pourquoi ils reçoivent vos messages. Nous vous recommandons d'envoyer un message de bienvenue leur rappelant qui vous êtes et pourquoi vous les contactez.

Lorsque vous recevez des réclamations, il est essentiel de réagir de manière appropriée en respectant les règles suivantes :

- Assurez-vous que l'adresse que vous utilisez pour recevoir des notifications de réclamation est en mesure de recevoir des e-mails. Pour en savoir plus sur la configuration des notifications de retour à l'expéditeur et de réclamation, consultez Configuration de notifications d'événement pour Amazon SES.
- Assurez-vous que vos notifications de réclamation ne sont pas marquées comme du courrier indésirable par votre FAI ou votre système de messagerie.
- Les notifications de réclamation contiennent généralement le corps de l'e-mail ; elles sont différentes des notifications de retour à l'expéditeur qui ne comprennent que les en-têtes d'e-mail. Par contre, dans les notifications de réclamation, l'adresse e-mail de la personne à l'origine de la réclamation est supprimée. Utilisez des en-têtes X personnalisés ou des identifiants spéciaux intégrés dans le corps de l'e-mail pour vous permettre d'identifier l'adresse e-mail qui émis la

réclamation. Cette technique facilite l'identification des adresses à l'origine des réclamations afin de les supprimer de vos listes de destinataires.

Qualité des messages

Les serveurs de messagerie utilisent des filtres de contenu pour détecter certains attributs dans vos messages permettant de déterminer si ces derniers sont légitimes. Ces filtres de contenu vérifient automatiquement le contenu de vos messages pour identifier les caractéristiques communes des messages indésirables ou malveillants. Amazon SES utilise des technologies de filtrage de contenu pour aider à détecter et à bloquer les messages contenant des programmes malveillants avant qu'ils ne soient envoyés.

Si les filtres de contenu d'un serveur de messagerie déterminent que votre message contient les caractéristiques d'un courrier indésirable ou d'un e-mail malveillant, votre message sera très probablement marqué et écarté des boîtes de réception de vos destinataires.

Gardez à l'esprit les points suivants lorsque vous concevez vos e-mails :

- Les filtres de contenu modernes sont intelligents, et s'adaptent et évoluent en permanence. Ils ne s'appuient pas sur un ensemble de règles prédéfini. Des services tiers comme ReturnPath ou Litmus peuvent vous aider à identifier les contenus de vos e-mails pouvant déclencher des filtres de contenu.
- Si vos e-mails contiennent des liens, vérifiez l'URL de ces liens par rapport aux listes DNSBL (DNS-based Blackhole Lists) comme celles figurant sur URIBL.com et SURBL.org.
- Évitez d'utiliser des raccourcisseurs de lien. Des expéditeurs malveillants peuvent utiliser des raccourcisseurs de lien pour masquer la destination effective d'un lien. Lorsque des FAI remarquent que des services de raccourcissement de lien, même les plus réputés, sont utilisés à des fins malfaisantes, ils peuvent refuser complètement l'accès à ces services. Si vos e-mails contiennent un lien vers un service de raccourcissement de lien en liste de refus, ils n'arriveront pas dans les boîtes de réception de vos clients, ce qui peut nuire à votre campagne d'e-mail.
- Testez chaque lien de vos e-mails pour vous assurer que celui-ci pointe vers la page prévue.
- Veillez à ce que votre site web comprenne des documents de politique de confidentialité et de conditions d'utilisation, et que ces documents soient à jour. Il est recommandé d'inclure un lien vers ces documents dans chaque e-mail que vous envoyez. En fournissant des liens vers ces documents, vous démontrez que vous n'avez rien à cacher à vos clients, ce qui peut aider à bâtir une relation de confiance.

- Si vous envisagez d'envoyer du contenu à haute fréquence (par exemple, des messages avec des « offres quotidiennes »), faites en sorte que celui-ci soit différent chaque jour. Lorsque vous envoyez des messages à haute fréquence, vous devez vous assurer que ces messages sont à jour et pertinents, et non répétitifs et agaçants.

Conseils et bonnes pratiques

Même lorsque vous avez l'intérêt de vos clients à l'esprit, vous pouvez être confronté à des situations qui ont un impact négatif sur la délivrabilité de vos messages. Les sections suivantes contiennent des recommandations qui vous aideront à vous assurer que vos communications par e-mail atteignent le public visé.

Recommandations générales

- Mettez-vous à la place de vos clients. Demandez-vous si le message que vous envoyez est un message que vous aimeriez recevoir dans votre boîte de réception. Si la réponse à cette question n'est pas un « oui » enthousiaste, il vaut mieux ne pas envoyer le message.
- Certains secteurs ont une réputation de mauvaise qualité, voire de pratiques d'e-mails malveillants. Si vous êtes impliqués dans les secteurs suivants, vous devez surveiller étroitement votre réputation et résoudre les problèmes immédiatement :
  - Prêts hypothécaires
  - Crédits
  - Produits pharmaceutiques et compléments alimentaires
  - Alcool et tabac
  - Divertissement pour adulte
  - Casinos et jeu
  - Programmes de travail à domicile

Considérations relatives à l'adresse d'expédition

- Réfléchissez bien aux adresses à partir desquelles vous envoyez des e-mails. L'adresse d'expédition (« From ») est l'une des premières informations que voient vos destinataires et celle-ci peut laisser une première impression durable. De plus, certains FAI associent votre réputation avec votre adresse d'expédition.

- Envisagez d'utiliser des sous-domaines pour les différents types de communications. Par exemple, supposons que vous envoyez des e-mails depuis le domaine exemple.com, et que vous prévoyez d'envoyer des messages marketing et des messages transactionnels. Plutôt que d'envoyer tous vos messages depuis exemple.com, envoyez vos messages marketing à partir d'un sous-domaine, par exemple, marketing.exemple.com, et vos messages transactionnels à partir d'un autre sous-domaine, comme commandes.exemple.com. Des sous-domaines distincts développent leur propre réputation. L'utilisation de sous-domaines réduit le risque d'atteinte à votre réputation si, par exemple, vos communications marketing atterrissent dans un piège à courrier indésirable ou déclenchent un filtre de contenu.
- Si vous prévoyez d'envoyer un grand nombre de messages, n'envoyez pas ces messages depuis une adresse basée sur un FAI, comme expéditeur@hotmail.com. Si un FAI détecte un volume important de messages depuis expéditeur@hotmail.com, ces e-mails ne sont pas traités comme ceux provenant d'un domaine d'envoi d'e-mail sortant que vous possédez.
- Travaillez avec le bureau de registre de votre domaine pour vous assurer que les informations WHOIS pour votre domaine sont exactes. Le fait de gérer un registre WHOIS honnête et à jour démontre que vous accordez de l'importance à la transparence et permet aux utilisateurs de déterminer rapidement si votre domaine est légitime.
- Évitez d'utiliser une adresse no-reply, comme no-reply@exemple.com, en tant qu'adresse d'expédition (« From ») ou adresse de réponse (« Reply-to »). L'utilisation d'une adresse e-mail no-reply@ envoie un message clair à vos destinataires : vous ne leur permettez pas de vous contacter et vous n'êtes pas intéressé par leurs commentaires.

Authentification

- Authentifiez votre domaine avec SPF et SenderID. Ces méthodes d'authentification confirment aux destinataires que chaque e-mail que vous envoyez provient effectivement du domaine indiqué.
- Signez vos messages sortants avec DKIM. Cette étape permet de confirmer aux destinataires que le contenu n'a pas été modifié lors de son transit entre l'expéditeur et le destinataire.
- Vous pouvez tester vos paramètres d'authentification SPF et DKIM en envoyant un message à une adresse e-mail basée sur un FAI que vous possédez, par exemple, un compte Gmail ou Hotmail personnel, puis en affichant les en-têtes du message. Les en-têtes indiquent si votre tentative d'authentification et de signature du message ont réussi.

Création et gestion de vos listes

- Mettez en place une stratégie de confirmation de l'acceptation. Lorsque des utilisateurs s'inscrivent pour recevoir des e-mails de votre part, envoyez-leur un message avec un lien de confirmation, et ne commencez pas à leur envoyer des e-mails tant qu'ils n'ont pas confirmé leur adresse en cliquant sur ce lien. Une stratégie de confirmation de l'acceptation contribue à réduire le nombre de messages d'erreur définitifs résultant d'erreurs typographiques.
- Lors de la collecte d'adresses e-mail avec un formulaire web, effectuez une validation minimale de ces adresses lors de la soumission. Par exemple, assurez-vous que les adresses que vous collectez sont correctement formées (qu'elles sont au format destinataire@exemple.com) et qu'elles font référence à des domaines avec des registres MX valides.
- Soyez vigilant lorsque vous permettez à une entrée définie par l'utilisateur d'être transmise sans être vérifiée à Amazon SES. Les inscriptions à des forums et les soumissions de formulaire présentent des risques spécifiques parce que le contenu est entièrement généré par l'utilisateur, et des expéditeurs de courrier indésirable peuvent remplir des formulaires avec leur propre contenu. Il vous incombe de vous assurer d'envoyer uniquement des e-mails avec un contenu de haute qualité.
- Il est très improbable qu'un alias standard (comme postmaster@, abuse@ ou noc@) s'inscrive volontairement pour vos e-mails. Veillez à n'envoyer des messages qu'à des personnes réelles qui veulent effectivement en recevoir. Cette règle s'applique tout spécialement aux alias standard qui sont généralement réservés à la surveillance des e-mails. Ces alias peuvent être ajoutés de façon malveillante à votre liste en tant que forme de sabotage visant à nuire à votre réputation.

Conformité d'

- Ayez à l'esprit les lois et réglementations s'appliquant aux messages marketing et à la lutte contre le courrier indésirable dans les pays et les régions vers lesquels vous envoyez des e-mails. Vous devez vous assurer que l'e-mail que vous envoyez est conforme à ces lois. Le présent guide ne couvre pas ces lois. Il est donc important que vous les recherchiez. Pour obtenir une liste des lois, consultez la législation anti-courrier indésirable par pays sur Wikipédia.
- Consultez toujours un avocat pour obtenir des conseils juridiques.

Utilisation d'Amazon SES avec un AWS SDK

AWS des kits de développement logiciel (SDK) sont disponibles pour de nombreux langages de programmation populaires. Chaque SDK fournit une API, des exemples de code et de la documentation qui facilitent la création d'applications par les développeurs dans leur langage préféré.

Documentation SDK	Exemples de code
AWS SDK for C++	AWS SDK for C++ exemples de code
AWS CLI	AWS CLI exemples de code
AWS SDK for Go	AWS SDK for Go exemples de code
AWS SDK for Java	AWS SDK for Java exemples de code
AWS SDK for JavaScript	AWS SDK for JavaScript exemples de code
Kit AWS SDK pour Kotlin	Kit AWS SDK pour Kotlin exemples de code
AWS SDK for .NET	AWS SDK for .NET exemples de code
AWS SDK for PHP	AWS SDK for PHP exemples de code
AWS Tools for PowerShell	Outils pour des exemples PowerShell de code
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) exemples de code
AWS SDK for Ruby	AWS SDK for Ruby exemples de code
Kit AWS SDK pour Rust	Kit AWS SDK pour Rust exemples de code
AWS SDK pour SAP ABAP	AWS SDK pour SAP ABAP exemples de code
Kit AWS SDK pour Swift	Kit AWS SDK pour Swift exemples de code

Pour des exemples spécifiques à Amazon SES, veuillez consulter Exemples de code pour Amazon SES utilisant des kits SDK AWS.

Exemple de disponibilité

Vous n’avez pas trouvé ce dont vous avez besoin ? Demandez un exemple de code en utilisant le lien Provide feedback (Fournir un commentaire) en bas de cette page.

Mise en route avec Amazon Simple Email Service

Ce chapitre présente les tâches nécessaires à la configuration initiale d'Amazon SES ainsi que des didacticiels pour vous aider à démarre.

Rubriques

Configuration d'Amazon Simple Email Service

Avant de commencer à utiliser Amazon SES, vous devez effectuer les tâches suivantes.

Tâches

Inscrivez-vous pour AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d‘inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l‘utilisateur racine a accès à l‘ensemble des Services AWS et des ressources de ce compte. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et

utilisez uniquement l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

Configuration de votre compte SES

Pour commencer avec SES, vérifiez une adresse e-mail et un domaine d'envoi de manière à pouvoir commencer à envoyer des e-mails via SES, puis demandez un accès en production pour votre compte à l'aide de l'assistant de configuration de compte SES.

Configuration de votre compte à l'aide de l'assistant de configuration de compte SES

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Sélectionnez Commencez sur la page d'accueil de la console SES pour être accompagné par l'assistant tout le long de la procédure de configuration de votre compte SES.

L' assistant de configuration de compte SES ne s'affiche que si vous n'avez pas encore créé d'identité (adresse e-mail ou domaine) dans SES.

Octroi d'un accès par programmation (pour interagir avec SES en dehors de la console)

Les utilisateurs ont besoin d'un accès programmatique s'ils souhaitent interagir avec AWS l'extérieur du AWS Management Console. La manière d'accorder un accès programmatique dépend du type d'utilisateur qui y accède AWS.

Pour accorder aux utilisateurs un accès programmatique, choisissez l’une des options suivantes.

Quel utilisateur a besoin d’un accès programmatique ?	Pour	Par
Identité de la main-d’œuvre (Utilisateurs gérés dans IAM Identity Center)	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées	Suivez les instructions de l’interface que vous souhaitez utiliser. • Pour le AWS CLI, voir Configuration du AWS

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
	aux AWS CLI AWS SDK ou AWS aux API.	CLI à utiliser AWS IAM Identity Center dans le guide de AWS Command Line Interface l'utilisateur. • Pour les AWS SDK, les outils et les AWS API, consultez la section Authentification IAM Identity Center dans le Guide de référence AWS des SDK et des outils.
IAM	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de la section Utilisation d'informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer les AWS CLI demandes programmatiques adressées aux AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour le AWS CLI, voir Authentification à l'aide des informations d'identification utilisateur IAM dans le Guide de l'AWS Command Line Interface utilisateur. • Pour les AWS SDK et les outils, voir Authentifier à l'aide d'informations d'identification à long terme dans le Guide de AWS référence des SDK et des outils. • Pour les AWS API, consultez la section Gestion des clés d'accès pour les utilisateurs IAM dans le guide de l'utilisateur IAM.

Téléchargez un AWS SDK (pour utiliser les API SES)

Pour appeler les API SES sans avoir à gérer des détails de bas niveau tels que l'assemblage de requêtes HTTP brutes, vous pouvez utiliser un AWS SDK. Les AWS SDK fournissent des fonctions et des types de données qui encapsulent les fonctionnalités de SES et d'autres AWS services. Pour télécharger un AWS SDK, accédez à la section SDK. Après avoir téléchargé le SDK, créez un fichier d'informations d'identification partagé et spécifiez vos clés AWS d'accès.

Migrer vers Amazon SES depuis une autre solution d'envoi d'e-mails

Cette rubrique fournit une présentation des étapes à suivre si vous souhaitez déplacer votre solution d'envoi d'e-mails vers une solution hébergée sur site ou vers Amazon SES à partir d'une solution hébergée sur une instance EC2 Amazon.

Rubriques de cette section :

Étape 1. Vérifier votre domaine

Avant de pouvoir utiliser Amazon SES pour envoyer des e-mails, vous devez vérifier les identités à partir desquelles vous prévoyez d'envoyer des e-mails. Dans Amazon SES, une identité peut être une adresse e-mail ou un domaine entier. Lorsque vous vérifiez un domaine, vous pouvez utiliser Amazon SES pour envoyer des e-mails depuis n'importe quelle adresse sur ce domaine. Pour plus d'informations sur la vérification d'un domaine, veuillez consulter Création d'une identité de domaine.

Étape 2. Demander un accès de production

Lorsque vous commencez à utiliser Amazon SES, votre compte se trouve dans un environnement de test (sandbox). Pendant que votre compte est dans l'environnement de test (sandbox), vous ne pouvez envoyer des e-mails qu'à des adresses et domaines que vous avez vérifiés. En outre, il existe des restrictions sur le nombre de messages que vous pouvez envoyer par jour et le nombre que vous pouvez envoyer par seconde. Pour plus d'informations sur la demande d'accès à la production, veuillez consulter Demande d'accès à la production (sortie du sandbox d'Amazon SES).

Étape 3. Configurer les systèmes d'authentification de domaine

Vous pouvez configurer votre domaine pour qu'il utilise des systèmes d'authentification tels que DKIM et SPF. Cette étape est techniquement facultative. Cependant, en configurant DKIM ou SPF (ou

les deux) pour votre domaine, vous pouvez améliorer la délivrabilité de vos e-mails et augmenter la confiance que vos clients ont en vous. Pour plus d'informations sur la configuration de SPF, veuillez consulter Authentification d'e-mails avec SPF dans Amazon SES. Pour plus d'informations sur la configuration de DKIM, veuillez consulter Authentification d'e-mails avec DKIM dans Amazon SES.

Étape 4 : Générer vos informations d'identification SMTP

Si vous prévoyez d'envoyer des e-mails à l'aide d'une application qui utilise SMTP, vous devez générer des informations d'identification SMTP. Vos informations d'identification SMTP sont différentes des informations d'identification classiques d' AWS . Ces informations d'identification sont également uniques dans chaque AWS région. Pour plus d'informations sur l'obtention de vos informations d'identification SMTP, veuillez consulter Obtention des informations d'identification SMTP Amazon SES.

Étape 5. Connexion à un point de terminaison SMTP

Si vous utilisez un agent de transfert de messages tel que postfix ou sendmail, vous devez mettre à jour la configuration de cette application pour faire référence à un point de terminaison SMTP Amazon SES. Pour obtenir la liste complète des points de terminaison SMTP, veuillez consulter Connexion à un point de terminaison SMTP Amazon SES. Notez que les informations d'identification SMTP que vous avez créées à l'étape précédente sont associées à une AWS région spécifique. Vous devez vous connecter au point de terminaison SMTP dans la région dans laquelle vous avez créé les informations d'identification SMTP.

Étapes suivantes

À ce stade, vous êtes prêt à commencer à envoyer des e-mails en utilisant Amazon SES. Cependant, il y a quelques étapes facultatives que vous pouvez effectuer.

- Vous pouvez créer des jeux de configuration, qui sont des ensembles de règles appliqués aux e-mails que vous envoyez. Par exemple, vous pouvez utiliser des jeux de configuration pour spécifier l'endroit où les notifications sont envoyées lorsqu'un e-mail est remis, lorsqu'un destinataire ouvre un message ou clique sur un lien, lorsqu'un e-mail est renvoyé à l'expéditeur et lorsqu'un destinataire marque votre message comme spam. Pour plus d’informations, consultez Utilisation des jeux de configuration dans Amazon SES.
- Lorsque vous envoyez un e-mail via Amazon SES, il est important de contrôler les retours à l'expéditeur et les réclamations pour votre compte. Amazon SES inclut la page de la console des métriques de réputation que vous pouvez utiliser pour suivre les retours à l'expéditeur et

les réclamations pour votre compte. Pour plus d'informations, consultez Utilisation de métriques de réputation pour suivre les taux de retours à l'expéditeur et de réclamations.. Vous pouvez également créer des CloudWatch alarmes qui vous alertent lorsque ces taux deviennent trop élevés. Pour plus d'informations sur la création d' CloudWatch alarmes, consultezCréation d'alarmes de surveillance de réputation avec CloudWatch.

- Les clients qui envoient un grand volume d'e-mails, ou ceux qui souhaitent simplement avoir un contrôle total sur la réputation de leurs adresses IP, peuvent louer des adresses IP dédiées moyennant des frais mensuels supplémentaires. Pour plus d'informations, consultez Adresses IP dédiées pour Amazon SES.

Demande d'accès à la production (sortie du sandbox d'Amazon SES)

Afin d'éviter les fraudes et les abus, et de vous aider à protéger votre réputation en tant qu'expéditeur, nous appliquons certaines restrictions aux nouveaux comptes Amazon SES.

Nous plaçons tous les nouveaux comptes dans l'environnement de test (sandbox) Amazon SES. Le statut sandbox de votre compte est unique pour chacun Région AWS d'entre eux. Même si votre compte est dans l'environnement de test (sandbox), vous pouvez utiliser toutes les fonctions d'Amazon SES. Toutefois, lorsque votre compte se trouve dans l'environnement de test (sandbox), nous appliquons les restrictions suivantes à votre compte :

- Vous pouvez uniquement envoyer des e-mails à des adresses e-mail et des domaines vérifiés, ou au simulateur de boîte aux lettres Amazon SES.
- Vous pouvez envoyer un maximum de 200 messages dans une période de 24 heures.
- Vous pouvez envoyer 1 message par seconde au maximum.
- Concernant l'autorisation d'envoi, ni vous, ni l'expéditeur délégué ne pouvez envoyer des e-mails à des adresses e-mail non vérifiées.
- Pour une suppression au niveau du compte, les actions groupées et les appels d'API SES liés à la gestion des listes de suppression sont désactivés.

Lorsque votre compte est passé du sandbox à la production, vous pouvez envoyer un e-mail à n'importe quel destinataire, que l'adresse ou le domaine du destinataire soient vérifiés ou non. Cependant, vous devez toujours vérifier chaque identité utilisée en tant qu'adresse « De », « Source », « Expéditeur » ou « Return-Path (Chemin de retour) ».

Suivez les procédures décrites dans cette section pour demander que votre compte soit retiré du sandbox et mis en production.

> **Note**
>
> - Si vous n'avez pas encore créé d'identité (adresse e-mail ou domaine) dans SES, vous pouvez ignorer les procédures décrites sur cette page et demander un accès de production pour votre compte en utilisant l'assistant de configuration du compte SES. Consultez Configurer votre compte SES pour savoir comment accéder à l'assistant.
> - Si vous utilisez Amazon SES pour envoyer des e-mails à partir d'une instance EC2 Amazon, vous devrez peut-être également demander que la limitation soit supprimée du port 25 de votre instance EC2 Amazon. Pour plus d'informations, consultez Comment supprimer le régulateur sur le port 25 de mon instance EC2 ? dans le AWS Knowledge Center.

Pour demander un accès à la production (supprimer votre compte du bac à sable) à l'aide du AWS Management Console

1. Ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sélectionnez Tableau de bord du compte.
3. Dans la zone d'avertissement située en haut de la console indiquant « Your Amazon SES account is in the sandbox, Votre compte Amazon SES est dans l'environnement de test (sandbox) », à droite, sélectionnez Request production access (Demander un accès de production).
4. Dans le mode Détails du compte, sélectionnez l'option Marketing ou Transactional (Transactionnel) qui décrit le mieux la majorité des e-mails que vous allez envoyer.

   - E-mail marketing - Envoyé sur une one-to-many base à une liste ciblée de prospects ou de clients contenant du contenu marketing et promotionnel, par exemple pour effectuer un achat, télécharger des informations, etc.
   - Courrier électronique transactionnel - Envoyé sur une one-to-one base unique à chaque destinataire, généralement déclenché par une action de l'utilisateur, telle qu'un achat sur un site Web, une demande de réinitialisation de mot de passe, etc.
5. Dans Website URL (URL du site Web), entrez l'URL de votre site Web pour nous aider à mieux comprendre le type de contenu que vous prévoyez d'envoyer.

6. Dans Use case description (Description du cas d'utilisation), expliquez comment vous prévoyez d'utiliser Amazon SES pour envoyer des e-mails. Pour nous aider à traiter votre demande, vous devez répondre aux questions suivantes :

   - Comment prévoyez-vous de créer ou d'acquérir votre liste de diffusion ?
   - Comment prévoyez-vous de gérer les retours à l'expéditeur et les réclamations ?
   - Comment les destinataires peuvent-ils refuser de recevoir des e-mails de votre part ?
   - Comment avez-vous choisi le taux d'envoi ou le quota d'envoi que vous avez spécifié dans cette demande ?
7. Pour Additional contact (Autres contact), indiquez-nous où vous souhaitez recevoir des communications concernant votre compte. Il peut s'agir d'une liste séparée par des virgules et pouvant comporter jusqu'à quatre adresses e-mail.
8. Pour Preferred contact language (Langue de contact préférée), choisissez si vous souhaitez recevoir les communications en English (Anglais) ou Japanese (Japonais).
9. Dans Acknowledgement (Accusé de réception), cochez la case pour indiquer que vous acceptez que les e-mails ne soient envoyés qu'aux personnes qui en ont fait la demande explicite et confirmez que vous avez mis en place une procédure pour traiter les notifications de retour à l'expéditeur et de réclamation.
10. Choisissez le bouton Submit request (Soumettre la demande) et une bannière s'affichera pour confirmer que votre demande a été soumise et qu'elle est en cours d'examen.

Une fois que vous avez envoyé un examen des détails de votre compte, vous ne pouvez pas les modifier tant que l'examen n'est pas terminé. L' AWS Support équipe fournit une première réponse à votre demande dans les 24 heures.

Pour empêcher que nos systèmes soient utilisés pour envoyer des contenus indésirables ou malveillants, chaque demande est traitée avec soin. Si nous sommes en mesure de le faire, nous répondons à votre demande dans ce délai de 24 heures. En revanche, si nous avons besoin que vous nous fournissiez de plus amples informations, le traitement de votre demande peut prendre plus de temps. Nous pourrions ne pas être en mesure de traiter votre demande si votre cas d’utilisation n’est pas conforme à nos stratégies.

En option, vous pouvez également soumettre votre demande d'accès à la production à l'aide du AWS CLI. Soumettre votre demande à l'aide du AWS CLI est utile lorsque vous souhaitez demander un accès à la production pour un grand nombre d'identités ou lorsque vous souhaitez automatiser le processus de configuration d'Amazon SES.

Pour demander que votre compte soit retiré de l'environnement de test (sandbox) Amazon SES à l'aide de la AWS CLI

1. Prérequis : vous devez installer et configurer AWS CLI. Pour en savoir plus, veuillez consulter le Guide de l'utilisateur AWS Command Line Interface.
2. Sur la ligne de commande, entrez la commande suivante :

```
aws sesv2 put-account-details \
--production-access-enabled \
--mail-type TRANSACTIONAL \
--website-url https://example.com \
--use-case-description "Use case description" \
--additional-contact-email-addresses info@example.com \
--contact-language EN
```

   Dans la commande précédente, procédez comme suit :

   a. Remplacez *TRANSACTIONAL (TRANSACTIONNEL)* par le type d'e-mail que vous prévoyez d'envoyer via Amazon SES. Vous pouvez spécifier `TRANSACTIONAL` ou `PROMOTIONAL`. Si plusieurs valeurs s'appliquent, indiquez l'option qui s'applique à la majorité des e-mails que vous prévoyez d'envoyer.

   b. Remplacez *https://example.com* par l'URL de votre site web. Ces informations nous aident à mieux comprendre le type de contenu que vous prévoyez d'envoyer.

   c. Remplacez *Use case description (Description du cas d'utilisation)* par une description de la façon dont vous prévoyez d'utiliser Amazon SES pour envoyer des e-mails. Pour nous aider à traiter votre demande, vous devez répondre aux questions suivantes :

      i. Comment prévoyez-vous de créer ou d'acquérir votre liste de diffusion ?

      ii. Comment prévoyez-vous de gérer les retours à l'expéditeur et les réclamations ?

      iii. Comment les destinataires peuvent-ils refuser de recevoir des e-mails de votre part ?

      iv. Comment avez-vous choisi le taux d'envoi ou le quota d'envoi que vous avez spécifié dans cette demande ?

   d. Remplacez *info@example.com* par les adresses e-mail où vous souhaitez recevoir des communications concernant votre compte. Il peut s'agir d'une liste séparée par des virgules et pouvant comporter jusqu'à quatre adresses e-mail.

e. Remplacez *EN* par votre langue préférée. Vous pouvez spécifier `EN` pour l'anglais ou `JA` pour le japonais.

Une fois que vous avez envoyé un examen des détails de votre compte, vous ne pouvez pas les modifier tant que l'examen n'est pas terminé. L' AWS Support équipe fournit une première réponse à votre demande dans les 24 heures.

Pour empêcher que nos systèmes soient utilisés pour envoyer des contenus indésirables ou malveillants, chaque demande est traitée avec soin. Si nous sommes en mesure de le faire, nous répondons à votre demande dans ce délai de 24 heures. En revanche, si nous avons besoin que vous nous fournissiez de plus amples informations, le traitement de votre demande peut prendre plus de temps. Nous pourrions ne pas être en mesure de traiter votre demande si votre cas d’utilisation n’est pas conforme à nos stratégies.

Gestion de vos limites d'envoi Amazon SES

Votre compte Amazon SES possède un ensemble de quotas d'envoi, qui permettent de réguler le nombre d'e-mails que vous pouvez envoyer et la fréquence à laquelle vous pouvez les envoyer. L'envoi de quotas profite à tous les clients Amazon SES, car ils aident à maintenir la relation de confiance entre Amazon SES et les fournisseurs de messagerie. Les quotas d'envoi vous aident à augmenter progressivement votre activité d'envoi et à diminuer la probabilité que les fournisseurs de messagerie bloqueront vos e-mails en raison de pics soudains et imprévus de votre volume ou fréquence d'envoi d'e-mails.

Les quotas suivants s'appliquent à l'envoi d'e-mails via Amazon SES :

- Quota d'envoi – Nombre maximal d'e-mails que vous pouvez envoyer sur une période de 24 heures. Ce quota est calculé sur une période glissante. Chaque fois que vous essayez d'envoyer un e-mail, Amazon SES calcule le nombre d'e-mails que vous avez envoyés au cours des 24 heures précédentes. Tant que le nombre total d'e-mails envoyés au cours des dernières 24 heures est inférieur à ce maximum quotidien, votre demande d'envoi est acceptée et votre e-mail est envoyé.

  Si l'envoi d'un message dépasse le maximum quotidien de votre compte, votre appel à Amazon SES est rejeté.
- Taux d'envoi – Nombre maximal d'e-mails par seconde pouvant être acceptés par Amazon SES à partir de votre compte. Vous pouvez dépasser ce quota sur de courtes durées, mais pas sur une période prolongée.

  > **Note**
  >
  > Le taux d'acception de vos messages par Amazon SES peut être inférieur au taux d'envoi maximum de votre compte.
- Taille de message maximale (Mo) — Taille maximale de l'e-mail que vous pouvez envoyer. Cela inclut toutes les images et pièces jointes qui font partie de l'e-mail après l'encodage MIME. Par exemple, si vous joignez un fichier de 5 Mo, la taille de la pièce jointe dans l'e-mail après codage MIME sera de ~6,85 Mo (environ 137 % de la taille du fichier original).

> **Note**
>
> Nous vous recommandons de télécharger vos pièces jointes sur des lecteurs sur le cloud et d'inclure l'URL de la pièce jointe du lecteur en nuage afin de réduire la taille de l'e-mail et d'améliorer la délivrabilité. SES ne peut pas garantir que les e-mails volumineux aboutissent dans la boîte de réception du destinataire, car les différents serveurs de messagerie ont des stratégies variables en fonction de la taille.

Vos quotas d'envoi Amazon SES sont distincts pour chaque région AWS. Pour en savoir plus sur l'utilisation d'Amazon SES dans plusieurs régions AWS, consultez Régions et Amazon SES.

Lorsque votre compte se trouve dans l'environnement de test (sandbox) Amazon SES, vous pouvez envoyer seulement 200 messages par période de 24 heures et votre fréquence d'envoi maximale est d'un message par seconde. Lorsque vous soumettez une demande de suppression de votre compte de l'environnement de test (sandbox), vous pouvez également demander que vos quotas soient augmentés en même temps. Pour en savoir plus sur le retrait de votre compte de l'environnement de test (sandbox), consultez Demande d'accès à la production (sortie du sandbox d'Amazon SES).

Lorsque votre compte a été supprimé de l'environnement de test (sandbox), vous pouvez demander des augmentations de quota supplémentaires à tout moment en créant un nouveau dossier dans le Centre de support AWS. Pour plus d'informations, consultez Augmentation de vos quotas d'envoi Amazon SES.

> **Note**
>
> Les quotas d'envoi sont définis en fonction des destinataires et non des messages. Par exemple, un e-mail qui a 10 destinataires compte pour 10 dans votre quota. Cependant, nous ne recommandons pas d'envoyer un e-mail à plusieurs destinataires en un seul appel à l'opération d'API `SendEmail`, car si l'appel échoue, l'e-mail est rejeté dans sa globalité. Nous vous recommandons d'appeler `SendEmail` une fois pour chaque destinataire.

- Pour augmenter vos quotas d'envoi, veuillez consulter Augmentation de vos quotas d'envoi Amazon SES.
- Pour surveiller vos quotas d'envoi à l'aide de la console Amazon SES ou de l'API Amazon SES, consultez Surveillance de vos quotas d'envoi Amazon SES.

- Pour en savoir plus sur les erreurs que votre application reçoit lorsque vous avez atteint vos quotas d'envoi, consultez Erreurs liées aux quotas d'envoi pour votre compte Amazon SES.

Augmentation de vos quotas d'envoi Amazon SES

Les quotas de votre compte par région actuelle peuvent être augmentés.

Ressource	Quota par défaut	Description
Quota d'envoi	200	Nombre maximum d'emails que vous pouvez envoyer en 24 heures pour ce compte dans la Région AWS actuelle.
Taux d'envoi	1	Nombre maximal d'e-mails qu'Amazon SES peut accepter chaque seconde pour ce compte dans la Région AWS actuelle.

Augmentation automatique des quotas d'envoi

Lorsque votre compte est en dehors de l'environnement de test (sandbox) et que vous envoyez des e-mails de production de haute qualité, nous pouvons augmenter automatiquement les quotas d'envoi pour votre compte. Souvent, nous augmentons automatiquement ces quotas avant que vous en ayez réellement besoin.

Pour que vous soyez éligible à des augmentations automatiques de taux, les points suivants doivent être réunis :

- Vous envoyez des contenus de grande qualité que vos destinataires souhaitent recevoir – Envoyez le contenu que les destinataires veulent et attendent. Arrêtez d'envoyer des e-mails à des clients qui ne les ouvrent pas.
- Vous envoyez des contenus de production réels – L'envoi de messages de test à des adresses e-mail fictives peut avoir un impact négatif sur votre taux de retours à l'expéditeur et de réclamations. En outre, si vous envoyez des messages uniquement à des destinataires internes, il est difficile de déterminer si vous envoyez des contenus que les clients souhaitent recevoir. Par contre, lorsque

vous envoyez vos messages de production à des clients externes, nous pouvons évaluer avec précision vos pratiques d'envoi d'e-mails.

- Vous envoyez un quota proche de votre quota actuel – Pour bénéficier d'une augmentation automatique du quota, votre volume quotidien d'e-mails doit approcher régulièrement le maximum quotidien de votre compte sans le dépasser.
- Vous avez des taux de retour à l'expéditeur et de réclamation bas – Minimisez le nombre de retours à l'expéditeur et de réclamations que vous recevez. Un nombre de retours à l'expéditeur et de réclamations élevé peuvent avoir un impact négatif sur vos quotas d'envoi.

L'utilisateur a demandé des quotas d'envoi supplémentaires

Si vos quotas d'envoi actuels ne sont pas adaptés à vos besoins et que nous ne les avons pas augmentés automatiquement, vous pouvez demander une augmentation.

- Quota d'envoi ou taux d'envoi : les demandes d'augmentation pour l'un ou l'autre peuvent être soumises via la console AWS Service Quotas.

Pour demander une augmentation de vos quotas d'envoi Amazon SES à l'aide de la console Service Quotas.

1. Ouvrez la console Service Quotas.
2. Sélectionnez la région pour laquelle vous souhaitez une augmentation en utilisant la liste déroulante dans le coin supérieur droit de la console (à côté de votre numéro de compte).
3. Dans le panneau de navigation, choisissez Services AWS.
4. Choisissez Amazon Simple Email Service (SES).
5. Choisissez un quota et suivez les instructions pour demander une augmentation de quota.

> SLA de l'équipe AWS Support pour les types de demandes d'augmentation
>
> Pour empêcher que nos systèmes soient utilisés pour envoyer des contenus indésirables ou malveillants, chaque demande est traitée avec soin. Si nous sommes en mesure de le faire, nous répondons à votre demande dans les délais spécifiés ci-dessous pour le type d'augmentation demandé. En revanche, si nous avons besoin que vous nous fournissiez de plus amples informations, le traitement de votre demande peut prendre plus de temps. Nous

nous réservons le droit de ne pas traiter votre demande si votre cas d'utilisation n'est pas conforme à nos stratégies.

- Quota d'envoi ou taux d'envoi : jusqu'à 24 heures.

> **Note**
>
> Bien que la console Service Quotas soit disponible dans de nombreuses langues, la prise en charge réelle n'est fournie qu'en anglais.

Surveillance de vos quotas d'envoi Amazon SES

Vous pouvez surveiller vos quotas d'envoi à l'aide de la console Amazon SES ou via l'API Amazon SES, que ce soit en appelant l'interface Query (HTTPS) directement ou indirectement via un kit SDK AWS, l'AWS Command Line Interface ou la AWS Tools for Windows PowerShell.

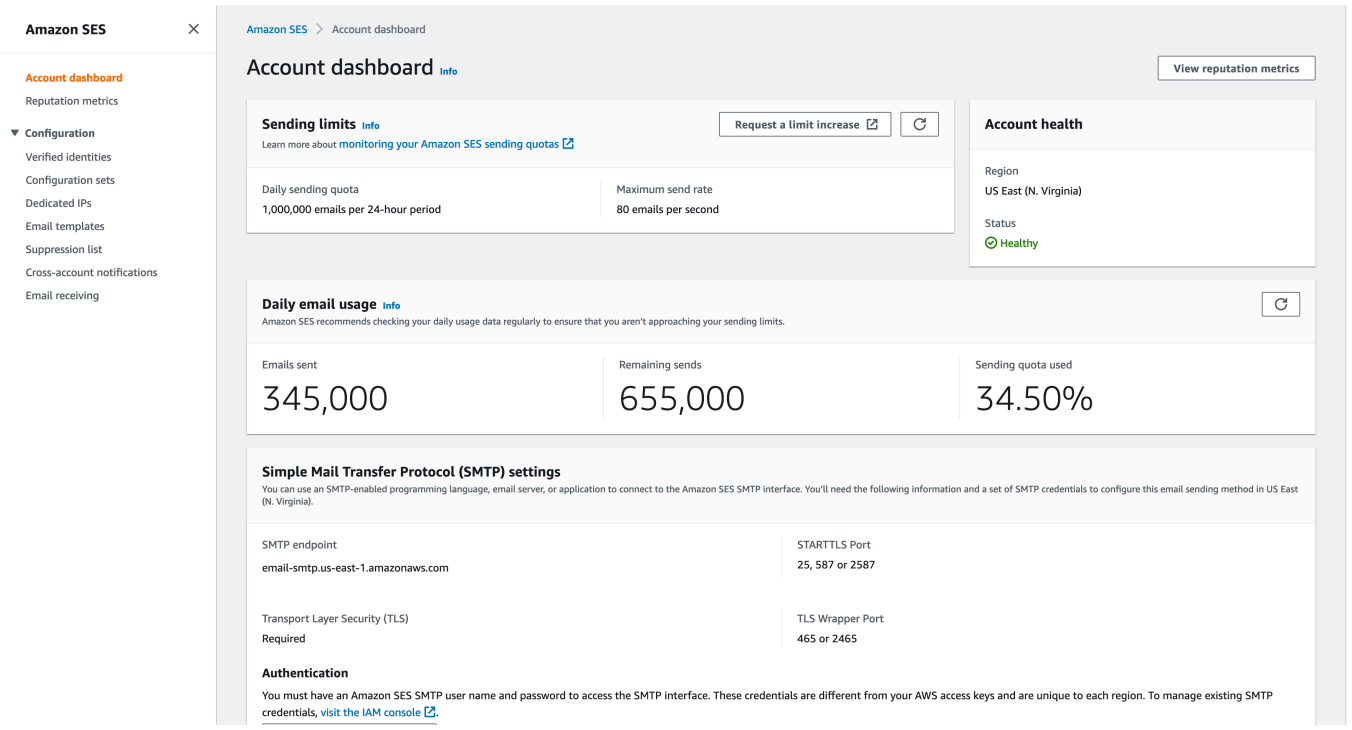
> **Important**
>
> Nous vous recommandons de vérifier fréquemment les statistiques d'envoi pour vous assurer que vous n'êtes pas près de vos quotas d'envoi. Si vous approchez la limite de vos quotas d'envoi, consultez Augmentation de vos quotas d'envoi Amazon SES Pour en savoir plus sur la façon de les augmenter. N'attendez pas d'avoir atteint vos quotas d'envoi pour envisager de les augmenter.

Surveillance de vos quotas d'envoi à l'aide de la console Amazon SES

La procédure suivante vous montre comment afficher vos quotas d'envoi à l'aide de la console Amazon SES.

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, choisissez Account dashboard (Tableau de bord du compte). Vos quotas d'envoi apparaissent sous Vos limites d'envoi. Le total des e-mails envoyés, les

envois restants et le pourcentage du quota d'envoi utilisé sont affichés sous Daily email usage (Utilisation quotidienne des e-mails).



3. Pour mettre à jour l'affichage, sélectionnez l'icône d'actualisation dans l'angle supérieur droit de l'onglet Daily email usage (Utilisation quotidienne des e-mails).

Surveillance de vos quotas d'envoi à l'aide de l'API Amazon SES

L'API Amazon SES fournit l'action `GetSendQuota`, qui renvoie vos quotas d'envoi. Lorsque vous appelez l'action `GetSendQuota`, vous recevez les informations suivantes :

- Nombre d'e-mails que vous avez envoyés au cours des 24 dernières heures
- Quota d'envoi pour la période en cours de 24 heures
- Taux d'envoi maximal

> **Note**
>
> Pour une description complète de `GetSendQuota`, veuillez consulter le document Référence de l'API Amazon Simple Email Service.

Erreurs liées aux quotas d'envoi pour votre compte Amazon SES

Si vous essayez d'envoyer un e-mail après avoir atteint votre quota d'envoi quotidien (le nombre maximal d'e-mails que vous pouvez envoyer sur une période de 24 heures) ou votre taux d'envois maximal (nombre maximal de messages que vous pouvez envoyer par seconde), Amazon SES supprime le message et ne tente pas de le remettre à nouveau. Amazon SES fournit également un message d'erreur qui explique le problème. La façon dont Amazon SES génère ce message d'erreur dépend de la façon dont vous avez tenté d'envoyer l'e-mail. Cette rubrique inclut des informations sur les messages que vous recevez via l'API Amazon SES et par le biais de l'interface SMTP.

Pour la technique à utiliser lorsque vous atteignez votre taux d'envoi maximum, consultez How to handle a « Throttling – Maximum sending rate exceeded » error (Comment traiter l'erreur « Restriction - Taux d'envoi maximum dépassé ») ? sur le blog AWS Targeting and Messaging (Ciblage et messagerie).

Atteinte des limites d'envoi avec l'API Amazon SES

Si vous essayez d'envoyer un e-mail à l'aide de l'API Amazon SES (ou d'un kit AWS SDK), mais que vous avez déjà dépassé les limites d'envoi de votre compte, l'API génère une erreur `ThrottlingException`. Le message d'erreur inclut l'un des messages suivants :

- `Daily message quota exceeded`
- `Maximum sending rate exceeded`

Si vous rencontrez une erreur de limitation, programmez votre application de telle sorte qu'elle attende un intervalle compris entre 0 et 10 minutes, puis réessayez la demande d'envoi.

Atteinte des limites d'envoi avec SMTP

Si vous essayez d'envoyer un e-mail à l'aide de l'interface SMTP Amazon SES, mais que vous avez déjà dépassé les limites d'envoi de votre compte, votre client SMTP peut afficher l'une des erreurs suivantes :

- `454 Throttling failure: Maximum sending rate exceeded`
- `454 Throttling failure: Daily message quota exceeded`

Les différents clients SMTP gèrent ces erreurs de diverses manières.

Configuration de l'envoi d'e-mails avec Amazon SES

Vous pouvez envoyer un e-mail avec Amazon Simple Email Service (Amazon SES) à l'aide de la console Amazon SES, de l'interface protocole SMTP (Simple Mail Transfer Protocol) d'Amazon SES ou de l'API Amazon SES. Vous utilisez généralement la console pour envoyer des e-mails de test et gérer votre activité d'envoi. Pour envoyer des e-mails en nombre, vous pouvez utiliser l'interface SMTP ou l'API. Pour en savoir plus sur la tarification des e-mails envoyés via Amazon SES, consultez Tarification d'Amazon SES.

- Si vous souhaitez utiliser un package logiciel, une application ou un langage de programmation compatible avec SMTP pour envoyer des e-mails via Amazon SES, ou intégrer Amazon SES à votre serveur de messagerie existant, utilisez l'interface SMTP Amazon SES. Pour plus d'informations, consultez Envoi d'un e-mail via l'interface SMTP Amazon SES par programmation.
- Si vous souhaitez appeler Amazon SES à l'aide de demandes HTTP brutes, utilisez l'API Amazon SES. Pour plus d'informations, consultez Utilisation de l'API Amazon SES pour envoyer un e-mail.

> **Important**
>
> Lorsque vous envoyez un e-mail à plusieurs destinataires (les destinataires sont les adresses figurant dans les zones « À », « Cc » et « Cci ») et que l'appel d'Amazon SES échoue, l'ensemble de l'e-mail est rejeté et aucun des destinataires ne reçoit l'e-mail concerné. Toutefois, nous vous recommandons d'envoyer un e-mail à un seul destinataire à la fois.

Utilisation de l'interface SMTP d'Amazon SES pour envoyer des e-mails

Pour envoyer un e-mail de production via Amazon SES, vous pouvez utiliser l'interface protocole SMTP (Simple Mail Transfer Protocol) ou l'API Amazon SES. Pour en savoir plus sur l'API Amazon SES, consultez Utilisation de l'API Amazon SES pour envoyer un e-mail. Cette section décrit l'interface SMTP.

Amazon SES envoie des e-mails à l'aide de SMTP, qui est le protocole de messagerie le plus courant sur Internet. Vous pouvez envoyer des e-mails via Amazon SES en utilisant différents langages

de programmation et logiciels compatibles avec SMTP pour vous connecter à l'interface SMTP Amazon SES. Cette section explique comment obtenir vos informations d'identification SMTP Amazon SES, comment envoyer des e-mails à l'aide de l'interface SMTP et comment configurer plusieurs logiciels et serveurs de messagerie afin d'utiliser Amazon SES pour envoyer des e-mails.

Pour trouver des solutions aux problèmes courants que vous êtes susceptible de rencontrer lors de l'utilisation d'Amazon SES via son interface SMTP, consultez Problèmes SMTP Amazon SES.

Conditions requises pour envoyer des e-mails via SMTP

Pour envoyer des e-mails à l'aide de l'interface SMTP Amazon SES, vous aurez besoin des éléments suivants :

- Adresse du point de terminaison SMTP. Pour obtenir la liste des points de terminaison SMTP Amazon SES, consultez Connexion à un point de terminaison SMTP Amazon SES.
- Le numéro de port de l'interface SMTP. Le numéro de port varie selon la méthode de connexion. Pour plus d'informations, consultez Connexion à un point de terminaison SMTP Amazon SES.
- Un nom d'utilisateur et un mot de passe SMTP. Les informations d'identification SMTP sont uniques pour chaque région AWS . Si vous prévoyez d'utiliser l'interface SMTP pour envoyer des e-mails dans plusieurs régions AWS , vous avez besoin d'informations d'identification SMTP pour chaque région.

  > **Important**
  >
  > Vos informations d'identification SMTP ne sont pas identiques à vos clés d' AWS accès ou à celles que vous utilisez pour vous connecter à la console Amazon SES. Pour plus d'informations sur la manière de générer vos informations d'identification SMTP, consultez Obtention des informations d'identification SMTP Amazon SES.

- Un logiciel client capable de communiquer à l'aide du protocole TLS (Transport Layer Security). Pour plus d'informations, consultez Connexion à un point de terminaison SMTP Amazon SES.
- Une adresse e-mail que vous avez vérifiée auprès d'Amazon SES. Pour plus d'informations, consultez Identités vérifiées dans Amazon SES.
- Augmentation des quotas d'envoi, si vous souhaitez envoyer de grandes quantités d'e-mails. Pour plus d'informations, consultez Gestion de vos limites d'envoi Amazon SES.

Méthodes d'envoi d'e-mails via SMTP

Vous pouvez envoyer des e-mails via SMTP par l'une des méthodes suivantes :

- Pour configurer ces logiciels compatibles avec SMTP de façon à envoyer des e-mails via l'interface SMTP Amazon SES, consultez Envoi d'e-mails via Amazon SES à l'aide de packages logiciels.
- Pour programmer une application de façon à envoyer des e-mails via Amazon SES, consultez Envoi d'un e-mail via l'interface SMTP Amazon SES par programmation.
- Pour configurer un serveur de messagerie existant de façon à envoyer tous vos messages sortants via Amazon SES, consultez Intégration d'Amazon SES à votre serveur de messagerie existant.
- Pour interagir avec l'interface SMTP Amazon SES à l'aide de la ligne de commande, ce qui peut être utile pour les tests, consultez Test de votre connexion à l'interface SMTP Amazon SES à l'aide de la ligne de commande.

Pour obtenir la liste des codes de réponse SMTP, consultez Codes de réponse SMTP renvoyés par Amazon SES.

Informations à fournir pour les e-mails

Lorsque vous accédez à Amazon SES via l'interface SMTP, votre application cliente SMTP assemble le message de façon à ce que les informations à fournir dépendent de l'application que vous utilisez. Un échange SMTP entre un client et un serveur nécessite au minimum les éléments suivants :

- Une adresse source
- Une adresse de destination
- Des données de message

Si vous utilisez l'interface SMTP et que le transfert de commentaires est activé, les retours à l'expéditeur, les réclamations et les notifications de livraison sont envoyées à l'adresse de l'expéditeur du message. Toute adresse « Répondre à » que vous spécifiez n'est pas utilisée.

Obtention des informations d'identification SMTP Amazon SES

Vous avez besoin des identifiants SMTP d'Amazon SES pour accéder à l'interface SMTP de SES.

Les informations d'identification que vous utilisez pour envoyer des e-mails via l'interface SMTP de SES sont uniques à chaque AWS région. Si vous utilisez l'interface SMTP SES pour envoyer des e-mails dans plusieurs régions, vous devez générer un ensemble d'informations d'identification d'identification SMTP pour chaque région que vous prévoyez d'utiliser.

Votre mot de passe SMTP est différent de votre clé d'accès AWS secrète. Pour en savoir plus sur les informations d'identification, consultez Types d'informations d'identification Amazon SES.

> **Note**
>
> Les points de terminaison SMTP ne sont actuellement pas disponibles en Afrique (Le Cap), en Asie-Pacifique (Jakarta), en Europe (Milan), en Israël (Tel Aviv) et au Moyen-Orient (Bahreïn).

Obtention d'informations d'identification SMTP SES à l'aide de la console SES

Lorsque vous utilisez le flux de travail SES ci-dessous pour générer des informations d'identification SMTP au moyen de la console, vous êtes dirigé vers la console IAM pour y créer un utilisateur avec les stratégies appropriées à l'appel de SES et les informations d'identification SMTP associées à cet utilisateur vous sont fournies.

Exigence

Un utilisateur IAM peut créer des informations d'identification SMTP SES, mais la stratégie de l'utilisateur doit disposer d'une autorisation d'utilisation d'IAM, car les informations d'identification SMTP SES sont créées via IAM. Votre stratégie IAM doit vous permettre d'exécuter les actions IAM suivantes : `iam:ListUsers`, `iam:CreateUser`, `iam:CreateAccessKey`, et `iam:PutUserPolicy`. Si vous essayez de créer des informations d'identification SMTP SES à l'aide de la console et que votre utilisateur IAM ne dispose pas de ces autorisations, un message d'erreur indiquant que votre compte n'est « pas autorisé à exécuter iam : » s'affiche. ListUsers

Pour créer vos informations d'identification SMTP

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Choisissez SMTP settings (Paramètres SMTP) dans le panneau de navigation de gauche pour ouvrir la page des paramètres du protocole SMTP (Simple Mail Transfer Protocol).

3. Choisissez Create SMTP Credentials (Création des informations d'identification SMTP) en haut à droite : la console IAM s'ouvre.
4. (Facultatif) Si vous devez afficher, modifier ou supprimer des utilisateurs SMTP que vous avez déjà créés, choisissez Manage my existing SMTP credentials (Gérer mes informations d'identification SMTP existantes) en bas à droite : la console IAM s'ouvre. Les détails relatifs à la gestion des informations d'identification SMTP sont fournis en suivant ces procédures.
5. Pour Créer un utilisateur pour SMTP, saisissez un nom d'utilisateur SMTP dans le champ Nom d'utilisateur. Vous pouvez également utiliser la valeur par défaut qui est fourni dans ce champ. Lorsque vous avez terminé, sélectionnez Créer un utilisateur dans le coin inférieur droit.
6. Sélectionnez Afficher sous Mot de passe SMTP – vos informations d'identification SMTP s'affichent à l'écran.
7. Téléchargez ces informations d'identification en sélectionnant Télécharger le fichier .csv ou copiez-les et stockez-les en lieu sûr, car vous ne pourrez plus les afficher ou les enregistrer après avoir fermé cette boîte de dialogue.
8. Choisissez Revenir à la console SES.

Vous pouvez afficher la liste des informations d'identification SMTP que vous avez créées à l'aide de cette procédure dans la console IAM sous Access management (Gestion des accès) et en choisissant Users (Utilisateurs) puis en utilisant la barre de recherche pour trouver tous les utilisateurs auxquels vous avez affecté des informations d'identification SMTP.

Vous pouvez également utiliser la console IAM pour supprimer des utilisateurs SMTP existants. Pour en savoir plus sur la suppression d'utilisateurs, consulte zGestion des utilisateurs IAM dans le Guide de mise en route IAM.

Si vous souhaitez modifier votre mot de passe SMTP, supprimez votre utilisateur SMTP existant dans la console IAM. Ensuite, effectuez les procédures ci-dessus pour générer un nouvel ensemble d'informations d'identification SMTP.

Obtention des informations d'identification SMTP SES en convertissant les informations d'identification existantes AWS

Si vous avez configuré un utilisateur à l'aide de l'interface IAM, vous pouvez déduire les informations d'identification SMTP SES de l'utilisateur à partir de ses AWS informations d'identification.

> **Important**
>
> N'utilisez pas d' AWS informations d'identification temporaires pour obtenir des informations d'identification SMTP. L'interface SMTP SES ne prend pas en charge les informations d'identification SMTP qui ont été générées à partir d'informations d'identification de sécurité temporaires.

Pour permettre à l'utilisateur IAM d'envoyer des e-mails à l'aide de l'interface SMTP SES, procédez de la façon suivante :

- Dérivez les informations d'identification SMTP de l'utilisateur à partir de ses AWS informations d'identification à l'aide de l'algorithme fourni dans cette section. Comme vous partez des AWS informations d'identification, le nom d'utilisateur SMTP est identique à l'ID de la clé AWS d'accès. Il vous suffit donc de générer le mot de passe SMTP.
- Appliquez la stratégie suivante à l'utilisateur IAM :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ses:SendRawEmail",
            "Resource": "*"
        }
    ]
}
```

Pour plus d'informations sur l'utilisation de SES avec IAM, consultez Gestion des identités et des accès dans Amazon SES.

> **Note**
>
> Bien que vous puissiez générer des informations d'identification SMTP SES pour tout utilisateur IAM, nous vous recommandons de créer un utilisateur IAM distinct lorsque vous générez vos informations d'identification SMTP. Pour en savoir plus sur les raisons pour

lesquelles il est recommandé de créer des utilisateurs à des fins spécifiques, consultez Bonnes pratiques IAM.

Le pseudocode suivant montre l'algorithme qui convertit une clé d'accès AWS secrète en mot de passe SMTP SES.

```
// Modify this variable to include your AWS secret access key
key = "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY";

// Modify this variable to refer to the AWS Region that you want to use to send email.
region = "us-west-2";

// The values of the following variables should always stay the same.
date = "11111111";
service = "ses";
terminal = "aws4_request";
message = "SendRawEmail";
version = 0x04;

kDate = HmacSha256(date, "AWS4" + key);
kRegion = HmacSha256(region, kDate);
kService = HmacSha256(service, kRegion);
kTerminal = HmacSha256(terminal, kService);
kMessage = HmacSha256(message, kTerminal);
signatureAndVersion = Concatenate(version, kMessage);
smtpPassword = Base64(signatureAndVersion);
```

Certains langages de programmation incluent des bibliothèques que vous pouvez utiliser pour convertir une clé d'accès secrète IAM en mot de passe SMTP. Cette section inclut un exemple de code que vous pouvez utiliser pour convertir une clé d'accès AWS secrète en mot de passe SMTP SES à l'aide de Python.

> **Note**
>
> L'exemple suivant utilise des f-strings qui ont été introduites dans Python 3.6 ; si vous utilisez une version plus ancienne, elles ne fonctionneront pas.
> Actuellement, le SDK Python (Boto3) prend officiellement en charge les versions 2.7 et 3.6 (ou ultérieures). Cependant, le support pour la version 2.7 est obsolète et sera supprimé le 15/07/2021. Vous devrez donc effectuer une mise à niveau vers la version 3.6 au minimum.

Python

```
#!/usr/bin/env python3

import hmac
import hashlib
import base64
import argparse

SMTP_REGIONS = [
    "us-east-2",  # US East (Ohio)
    "us-east-1",  # US East (N. Virginia)
    "us-west-2",  # US West (Oregon)
    "ap-south-1",  # Asia Pacific (Mumbai)
    "ap-northeast-2",  # Asia Pacific (Seoul)
    "ap-southeast-1",  # Asia Pacific (Singapore)
    "ap-southeast-2",  # Asia Pacific (Sydney)
    "ap-northeast-1",  # Asia Pacific (Tokyo)
    "ca-central-1",  # Canada (Central)
    "eu-central-1",  # Europe (Frankfurt)
    "eu-west-1",  # Europe (Ireland)
    "eu-west-2",  # Europe (London)
    "eu-south-1",  # Europe (Milan)
    "eu-north-1",  # Europe (Stockholm)
    "sa-east-1",  # South America (Sao Paulo)
    "us-gov-west-1",  # AWS GovCloud (US)
]

# These values are required to calculate the signature. Do not change them.
DATE = "11111111"
SERVICE = "ses"
MESSAGE = "SendRawEmail"
TERMINAL = "aws4_request"
VERSION = 0x04


def sign(key, msg):
    return hmac.new(key, msg.encode("utf-8"), hashlib.sha256).digest()


def calculate_key(secret_access_key, region):
    if region not in SMTP_REGIONS:
        raise ValueError(f"The {region} Region doesn't have an SMTP endpoint.")
```

```
    signature = sign(("AWS4" + secret_access_key).encode("utf-8"), DATE)
    signature = sign(signature, region)
    signature = sign(signature, SERVICE)
    signature = sign(signature, TERMINAL)
    signature = sign(signature, MESSAGE)
    signature_and_version = bytes([VERSION]) + signature
    smtp_password = base64.b64encode(signature_and_version)
    return smtp_password.decode("utf-8")


def main():
    parser = argparse.ArgumentParser(
        description="Convert a Secret Access Key to an SMTP password."
    )
    parser.add_argument("secret", help="The Secret Access Key to convert.")
    parser.add_argument(
        "region",
        help="The AWS Region where the SMTP password will be used.",
        choices=SMTP_REGIONS,
    )
    args = parser.parse_args()
    print(calculate_key(args.secret, args.region))


if __name__ == "__main__":
    main()
```

Pour obtenir votre mot de passe SMTP à l'aide de ce script, enregistrez le code précédent en tant que `smtp_credentials_generate.py`. Exécutez la ligne de commande suivante au moment de l'invite :

```
python path/to/smtp_credentials_generate.py wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY us-east-1
```

Dans la commande précédente, procédez comme suit :

- Remplacez *path/to/ (chemin/vers/)* par le chemin vers l'emplacement où vous avez enregistré `smtp_credentials_generate.py`.
- Remplacez *WJALRXUTNFEMI/K7MDENG/B PxRfi CYEXAMPLEKEY par la clé* d'accès secrète que vous souhaitez convertir en mot de passe SMTP.

- Remplacez *us-east-1* par la région dans laquelle vous souhaitez AWS utiliser les informations d'identification SMTP.

Lorsque ce script s'exécute correctement, la seule sortie est votre mot de passe SMTP.

Connexion à un point de terminaison SMTP Amazon SES

Pour envoyer un e-mail à l'aide de l'interface SMTP Amazon SES, vous devez vous connecter à un point de terminaison SMTP. Pour obtenir la liste complète des points de terminaison SMTP Amazon SES, veuillez consulter Points de terminaison et quotas Amazon Simple Email Service dans le document Références générales AWS.

Le point de terminaison SMTP Amazon SES nécessite que toutes les connexions soient chiffrées à l'aide du protocole TLS (Transport Layer Security). (Notez que le protocole TLS est souvent désigné par le nom de son prédécesseur, le protocole SSL.) Amazon SES prend en charge deux mécanismes d'établissement d'une connexion à chiffrement TLS : STARTTLS et TLS Wrapper. Consultez la documentation de votre logiciel pour déterminer s'il prend en charge STARTTLS, TLS Wrapper ou les deux.

Amazon Elastic Compute Cloud (Amazon EC2) limite par défaut le trafic des e-mails sur le port 25. Pour éviter les délais d'expiration lors de l'envoi d'e-mails via le point de terminaison SMTP à partir d'EC2, remplissez une Demande de suppression des limites d'envoi d'e-mails pour supprimer la limite. Vous pouvez également envoyer des e-mails à l'aide d'un autre port ou utiliser un point de terminaison d'un VPC Amazon.

Pour des problèmes de connexion SMTP, consultez Problèmes SMTP.

STARTTLS

STARTTLS est un moyen de mettre à niveau une connexion non chiffrée en connexion chiffrée. Il existe différentes versions de STARTTLS selon les protocoles. La version SMTP est définie dans RFC 3207.

Pour configurer une connexion STARTTLS, le client SMTP se connecte au point de terminaison SMTP Amazon SES sur le port 25, 587 ou 2587, émet une commande EHLO et attend que le serveur annonce qu'il prend en charge l'extension SMTP STARTTLS. Le client émet ensuite la commande STARTTLS afin de lancer la négociation TLS. Une fois la négociation terminée, le client émet une commande EHLO via la nouvelle connexion chiffrée et la session SMTP se poursuit normalement.

TLS Wrapper

TLS Wrapper (également connu sous le nom de SMTPS ou de protocole de négociation) est un moyen de lancer une connexion chiffrée sans commencer par établir une connexion non chiffrée. Avec TLS Wrapper, le point de terminaison SMTP Amazon SES n'effectue pas de négociation TLS : c'est la responsabilité du client de se connecter au point de terminaison à l'aide de TLS et de continuer à utiliser TLS pour la totalité de la conversation. TLS Wrapper est un protocole plus ancien, mais de nombreux clients continuent de le prendre en charge.

Pour configurer une connexion TLS Wrapper, le client SMTP se connecte au point de terminaison SMTP Amazon SES sur le port 465 ou 2465. Le serveur présente son certificat, le client émet une commande EHLO et la session SMTP se poursuit normalement.

Envoi d'e-mails via Amazon SES à l'aide de packages logiciels

Il existe un certain nombre de packages logiciels commerciaux ou open source qui prennent en charge l'envoi d'e-mails via SMTP. Voici quelques exemples :

- Plates-formes de création de blogs
- Agrégateurs RSS
- Logiciel de gestion de liste
- Systèmes de flux de travail

Vous pouvez configurer ces logiciels compatibles avec SMTP de façon à envoyer des e-mails via l'interface SMTP Amazon SES. Pour obtenir des instructions sur la configuration de SMTP pour un package logiciel spécifique, consultez la documentation du logiciel concerné.

La procédure suivante montre comment configurer l'envoi Amazon SES dans JIRA, une solution de suivi des problèmes connue. Avec cette configuration, JIRA peut avertir les utilisateurs par e-mail dès qu'un problème de logiciel change de statut.

Pour configurer JIRA de façon à envoyer un e-mail à l'aide d'Amazon SES

1. À l'aide de votre navigateur Web, connectez-vous à JIRA avec des informations d'identification de l'administrateur.
2. Dans la fenêtre du navigateur, choisissez Administration (Administration).
3. Dans le menu System (Système), choisissez Mail (e-mail).

4. Sur la page Mail administration (Administration des e-mails), choisissez Mail Servers (Serveurs des e-mails).
5. Choisissez Configure new SMTP mail server (Configurer un nouveau serveur de messagerie SMTP).
6. Sur l'écran Add SMTP Mail Server (Ajouter un serveur de messagerie SMTP), remplissez les champs suivants :

   a. Name (Nom) – Nom descriptif pour ce serveur.

   b. From address (Adresse d'origine) – Adresse à partir de laquelle l'e-mail de retour à l'expéditeur sera envoyé. Vous devez vérifier cette adresse e-mail avec Amazon SES avant de pouvoir l'utiliser pour envoyer des messages. Pour en savoir plus sur la vérification, consultez Identités vérifiées dans Amazon SES.

   c. Email prefix (Préfixe de l'e-mail) – Chaîne que JIRA ajoute à chaque ligne d'objet avant l'envoi.

   d. Protocol (Protocole) – Choisissez SMTP.

      > **Note**
      >
      > Si vous ne pouvez pas vous connecter à Amazon SES à l'aide de ce paramètre, essayez SECURE_SMTP.

   e. Host Name (Nom d'hôte) – Pour obtenir la liste des points de terminaison SMTP Amazon SES, consultez Connexion à un point de terminaison SMTP Amazon SES. Par exemple, si vous souhaitez utiliser le point de terminaison Amazon SES dans la région USA Ouest (Oregon), le nom d'hôte est email-smtp.us-west-2.amazonaws.com.

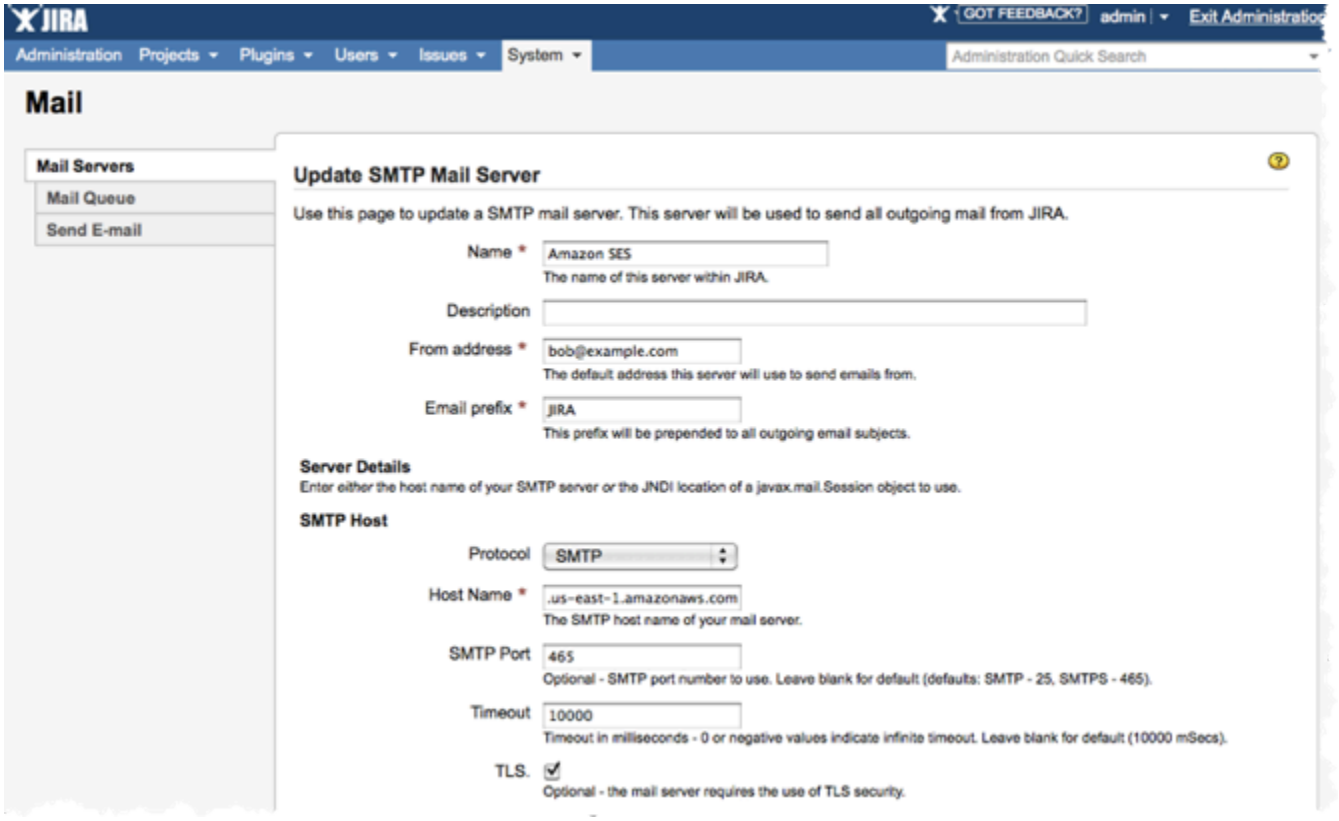
   f. SMTP port—25, 587 ou 2587 (pour vous connecter à l'aide de STARTTLS), ou 465 ou 2465 (pour vous connecter à l'aide de TLS Wrapper).

   g. TLS – Activez la case à cocher.

   h. User name (Nom d'utilisateur) – Votre nom d'utilisateur SMTP.

   i. Password (Mot de passe) – Votre mot de passe SMTP.

   Vous pouvez voir les paramètres pour TLS Wrapper dans l'image suivante.



7. Choisissez Test Connection (Connexion test). Si l'e-mail de test envoyé par JIRA via Amazon SES arrive correctement, cela indique que votre configuration est terminée.

Envoi d'un e-mail via l'interface SMTP Amazon SES par programmation

Pour envoyer un e-mail à l'aide de l'interface SMTP Amazon SES, vous pouvez utiliser un langage de programmation, un serveur de messagerie ou une application compatible avec SMTP. Avant de commencer, complétez les tâches dans Configuration d'Amazon Simple Email Service. Vous aurez également besoin d'obtenir les informations supplémentaires suivantes :

- Vos informations d'identification Amazon SMTP SES, qui vous permettent de vous connecter au point de terminaison Amazon SMTP SES. Pour obtenir vos informations d'identification SMTP Amazon SES, consultez Obtention des informations d'identification SMTP Amazon SES.

> **Important**
>
> Vos informations d'identification SMTP sont différentes de vos AWS informations d'identification. Pour en savoir plus sur les informations d'identification, consultez Types d'informations d'identification Amazon SES.

- Adresse du point de terminaison SMTP. Pour obtenir la liste des points de terminaison SMTP Amazon SES, consultez Connexion à un point de terminaison SMTP Amazon SES.
- Le numéro de port de l'interface SMTP Amazon SES, qui dépend de la méthode de connexion. Pour plus d'informations, consultez Connexion à un point de terminaison SMTP Amazon SES.

Intégration d'Amazon SES à votre serveur de messagerie existant

Si vous administrez actuellement votre propre serveur de messagerie, vous pouvez utiliser le point de terminaison SMTP Amazon SES pour envoyer tous vos e-mails sortants à Amazon SES. Il n'est pas nécessaire de modifier vos clients et applications de messagerie existants ; le passage à Amazon SES sera transparent pour eux.

Plusieurs Mail Transfer Agent (MTA) prennent en charge l'envoi d'e-mails via des relais SMTP. Cette section propose des conseils généraux sur la configuration de certains MTA couramment utilisés pour envoyer des e-mails à l'aide de l'interface SMTP Amazon SES.

Le point de terminaison SMTP Amazon SES nécessite que toutes les connexions soient chiffrées à l'aide du protocole TLS (Transport Layer Security).

Rubriques

- Intégration d'Amazon SES au serveur SMTP IIS de Microsoft Windows Server

Intégration d'Amazon SES au serveur SMTP IIS de Microsoft Windows Server

Vous pouvez configurer le serveur SMTP IIS de Microsoft Windows Server de façon à envoyer des e-mails via Amazon SES. Ces instructions ont été écrites à l'aide de Microsoft Windows Server 2012 sur une instance Amazon EC2. Vous pouvez utiliser la même configuration sur Microsoft Windows Server 2008 et Microsoft Windows Server 2008 R2.

> **Note**
>
> Windows Server est une application tierce qui n'est ni développée ni prise en charge par Amazon Web Services. Les procédures décrites dans cette section sont fournies à titre informatif seulement et peuvent être modifiées sans préavis.

Pour intégrer le serveur SMTP IIS de Microsoft Windows Server à Amazon SES

1. Commencez par configurer Microsoft Windows Server 2012 en suivant les instructions ci-dessous.

   a. Dans la console de gestion Amazon EC2, lancez une nouvelle Instance EC2 de base de Microsoft Windows Server 2012.

   b. Connectez-vous à l'instance et connectez-vous à l'aide de l'option Bureau à distance en suivant les instructions de Démarrer avec les instances Windows Amazon EC2.

   c. Lancez le tableau de bord du gestionnaire de serveur.

   d. Installez le rôle Serveur Web. Veillez à inclure les outils de compatibilité de gestion IIS 6 (une option sous la case à cocher Serveur Web).

   e. Installez la fonctionnalité Serveur SMTP.

2. Ensuite, configurez le service IIS SMTP en suivant les instructions ci-dessous.

   a. Revenez au tableau de bord du gestionnaire de serveur.

   b. Dans le menu Tools (Outils), choisissez Internet Information Services (IIS) 6.0 Manager (Gestionnaire des services Internet (IIS) 6.0).

   c. Cliquez avec le bouton droit de la souris sur Serveur virtuel SMTP n° 1, puis sélectionnez Propriétés.

   d. Sous l'onglet Accès, sous Restrictions de relais, choisissez Relais.

   e. Dans la boîte de dialogue Restrictions de relais, choisissez Ajouter.

   f. Sous Ordinateur unique, entrez 127.0.0.1 pour l'adresse IP. Vous disposez maintenant d'un accès à ce serveur pour transmettre des e-mails à Amazon SES via le service SMTP IIS.

      Dans cette procédure, nous supposons que vos e-mails sont générés sur ce serveur. Si l'application qui génère l'e-mail est exécutée sur un serveur distinct, vous devez accorder l'accès de relais pour ce serveur dans SMTP IIS.

      > **Note**
      >
      > Pour étendre le relais SMTP à des sous-réseaux privés, pour Relay Restriction (Restriction de relais), utilisez Single Computer (Ordinateur unique) 127.0.0.1 et Group of Computers (Groupe d'ordinateurs) 172.1.1.0 - 255.255.255.0, dans la section masque réseau (netmask). Pour Connection (Connexion), utilisez Ordinateur

unique 127.0.0.1 et Group of Computers (Groupe d'ordinateurs) 172.1.1.0 - 255.255.255.0, dans la section masque réseau (netmask).

3. Enfin, configurez le serveur de façon à envoyer des e-mails via Amazon SES en suivant les instructions ci-dessous.

   a. Revenez à la boîte de dialogue (SMTP Virtual Server #1 Properties) Propriétés du serveur virtuel SMTP n° 1, puis choisissez l'onglet Delivery (Remise).

   b. Sous l'onglet Delivery (Remise), choisissez Outbound Security (Sécurité sortante).

   c. Sélectionnez Basic Authentication (Authentification de base), puis saisissez vos informations d'identification SMTP Amazon SES. Vous pouvez obtenir ces informations d'identification à partir de la console Amazon SES à l'aide de la procédure Obtention des informations d'identification SMTP Amazon SES.

      ⚠ Important

      Vos informations d'identification SMTP ne sont pas identiques à votre identifiant de clé AWS d'accès et à votre clé d'accès secrète. N'essayez pas d'utiliser vos AWS informations d'identification pour vous authentifier auprès du point de terminaison SMTP. Pour en savoir plus sur les informations d'identification, consultez Types d'informations d'identification Amazon SES.

   d. Assurez-vous que TLS encryption (Chiffrement TLS) est sélectionné.

   e. Revenez à l'onglet Delivery (Remise).

   f. Choisissez Outbound Connections (Connexions sortantes).

   g. Dans la boîte de dialogue Outbound Connections (Connexions sortantes), assurez-vous que le port est 25 ou 587.

   h. Choisir Advanced (Avancé).

   i. Pour le nom Smart host (Hôte intelligent), entrez le point de terminaison Amazon SES que vous utiliserez (par exemple, email-smtp.us-west-2.amazonaws.com). Pour obtenir la liste des URL des points de terminaison Régions AWS où Amazon SES est disponible, consultez Amazon Simple Email Service (Amazon SES) dans le. Références générales AWS

   j. Revenez au tableau de bord du gestionnaire de serveur.

   k. Sur le tableau de bord du gestionnaire de serveur, cliquez avec le bouton droit de la souris sur Serveur virtuel SMTP n° 1, puis redémarrez le service de façon à récupérer la nouvelle configuration.

l. Envoyez un e-mail via ce serveur. Vous pouvez examiner les en-têtes de message afin de confirmer que celui-ci a été remis via Amazon SES.

Test de votre connexion à l'interface SMTP Amazon SES à l'aide de la ligne de commande

Vous pouvez utilisez les méthodes décrites dans cette section depuis la ligne de commande pour tester votre connexion au point de terminaison SMTP Amazon SES, valider vos informations d'identification SMTP et résoudre les problèmes de connexion. Ces procédures utilisent des outils et des bibliothèques qui sont inclus avec la plupart des systèmes d'exploitation courants.

Pour plus d'informations sur la résolution des problèmes de connexion SMTP, veuillez consulter Problèmes SMTP Amazon SES.

Prérequis

Lorsque vous vous connectez à l'interface SMTP Amazon SES, vous devez fournir un ensemble d'informations d'identification SMTP. Ces informations d'identification SMTP sont différentes de vos informations d' AWS identification standard. Les deux types d'informations d'identification ne sont pas interchangeables. Pour en savoir plus sur l'obtention de vos informations d'identification SMTP, consultez the section called “Obtention des informations d'identification SMTP”.

Test de votre connexion à l'interface SMTP Amazon SES

Vous pouvez utiliser la ligne de commande pour tester votre connexion à l'interface SMTP Amazon SES sans vous authentifier ni envoyer de messages. Cette procédure est utile pour résoudre les problèmes de connectivité de base. Si votre connexion de test échoue, consultez Problèmes SMTP.

Cette section inclut des procédures pour tester votre connexion à l'aide d'OpenSSL (qui est inclus dans la plupart des distributions Linux, macOS et Unix, et est également disponible pour Windows) et de `Test-NetConnection` l'applet de commande (incluse PowerShell dans les versions les plus récentes de Windows).

Linux, macOS, or Unix

Il existe deux façons de se connecter à l'interface SMTP Amazon SES avec OpenSSL : à l'aide du protocole SSL explicite sur le port 587 ou à l'aide du protocole SSL implicite sur le port 465.

Pour vous connecter à l'interface SMTP à l'aide du protocole SSL explicite

- Sur la ligne de commande, tapez la commande suivante afin de vous connecter au serveur SMTP Amazon SES :

```
openssl s_client -crlf -quiet -starttls smtp -connect email-smtp.us-
west-2.amazonaws.com:587
```

Dans la commande précédente, remplacez *email-smtp.us-west-2.amazonaws.com* par l'URL du point de terminaison SMTP Amazon SES pour votre AWS région. Pour plus d'informations, consultez the section called “Régions”.

Si la connexion est réussie, vous obtenez une sortie similaire à ce qui suit :

```
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = email-smtp.us-west-2.amazonaws.com
verify return:1
250 Ok
```

La connexion se ferme automatiquement au bout de 10 secondes d'inactivité.

Vous pouvez également utiliser le protocole SSL implicite pour vous connecter à l'interface SMTP via le port 465.

Pour vous connecter à l'interface SMTP à l'aide du protocole SSL implicite

- Sur la ligne de commande, tapez la commande suivante afin de vous connecter au serveur SMTP Amazon SES :

```
openssl s_client -crlf -quiet -connect email-smtp.us-west-2.amazonaws.com:465
```

Dans la commande précédente, remplacez *email-smtp.us-west-2.amazonaws.com* par l'URL du point de terminaison SMTP Amazon SES pour votre AWS région. Pour plus d'informations, consultez the section called “Régions”.

Si la connexion est réussie, vous obtenez une sortie similaire à ce qui suit :

```
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = email-smtp.us-west-2.amazonaws.com
verify return:1
220 email-smtp.amazonaws.com ESMTP SimpleEmailService-d-VCSHDP1YZ
 A1b2C3d4E5f6G7h8I9j0
```

La connexion se ferme automatiquement au bout de 10 secondes d'inactivité.

PowerShell

Vous pouvez utiliser l'NetConnectionapplet de commande Test-in PowerShell pour vous connecter au serveur SMTP Amazon SES.

> **Note**
>
> L'applet de commande `Test-NetConnection` peut déterminer si votre ordinateur peut se connecter au point de terminaison SMTP Amazon SES. Toutefois, il ne teste pas si votre ordinateur peut établir une connexion SSL implicite ou explicite au point de terminaison SMTP. Pour tester une connexion SSL, vous pouvez installer OpenSSL pour Windows pour envoyer un e-mail de test.

Pour vous connecter à l'interface SMTP à l'aide de l'applet de commande **`Test-NetConnection`**

- Dans PowerShell, entrez la commande suivante pour vous connecter au serveur SMTP Amazon SES :

  ```
  Test-NetConnection -Port 587 -ComputerName email-smtp.us-west-2.amazonaws.com
  ```

  Dans la commande précédente, remplacez *`email-smtp.us-west-2.amazonaws.com`* par l'URL du point de terminaison SMTP Amazon SES de votre AWS région, et remplacez *`587`* par le numéro de port. Pour en savoir plus sur les points de terminaison régionaux dans Amazon SES, consultez the section called “Régions”.

  Si la connexion aboutit, vous voyez une sortie similaire à l'exemple suivant :

```
ComputerName     : email-smtp.us-west-2.amazonaws.com
RemoteAddress    : 198.51.100.126
RemotePort       : 587
InterfaceAlias   : Ethernet
SourceAddress    : 203.0.113.46
TcpTestSucceeded : True
```

Utilisation de l'API Amazon SES pour envoyer un e-mail

Pour envoyer un e-mail de production via Amazon SES, vous pouvez utiliser l'interface protocole SMTP (Simple Mail Transfer Protocol) ou l'API Amazon SES. Pour en savoir plus sur l'interface SMTP, consultez Utilisation de l'interface SMTP d'Amazon SES pour envoyer des e-mails. Cette section décrit l'envoi d'e-mails à l'aide de l'API.

Lorsque vous envoyez un e-mail à l'aide de l'API Amazon SES, vous spécifiez le contenu du message et Amazon SES compose un e-mail MIME pour vous. Vous pouvez également assembler l'e-mail vous-même afin d'avoir un contrôle total sur le contenu du message. Pour de plus amples informations sur l'utilisation de l'API, veuillez consulter la Référence d'API Amazon Simple Email Service. Pour obtenir la liste des URL des points de terminaison Régions AWS où Amazon SES est disponible, consultez la section Points de terminaison et quotas Amazon Simple Email Service dans le. Références générales AWS

Vous pouvez appeler l'API des manières suivantes :

- Effectuer des demandes HTTPS directes – Il s'agit de la méthode la plus avancée, car vous devez manuellement gérer l'authentification et la signature de vos demandes, ainsi que la création des demandes. Pour en savoir plus sur l'API Amazon SES, consultez la page Welcome (Bienvenue) dans API v2 Reference (référence API v2).
- Utiliser un AWS SDK :AWS les SDK facilitent l'accès aux API de plusieurs AWS services, notamment Amazon SES. Lorsque vous utilisez un kit SDK, il s'occupe de l'authentification, de la signature des demandes, de la logique de nouvelle tentative, de la gestion des erreurs et d'autres fonctions de bas niveau, afin de vous permettre de vous concentrer sur le développement des applications qui raviront vos clients.
- Utiliser une interface de ligne de commande – L'AWS Command Line Interface est l'outil de ligne de commande pour Amazon SES. Nous proposons également les AWS outils PowerShell pour ceux qui écrivent des scripts dans l' PowerShellenvironnement.

Que vous accédiez à l'API Amazon SES directement ou indirectement par le biais d'un AWS SDK, AWS Command Line Interface ou des AWS outils pour PowerShell, l'API Amazon SES vous permet d'envoyer un e-mail de deux manières différentes, en fonction du degré de contrôle que vous souhaitez avoir sur la composition du message électronique :

- Mis en forme – Amazon SES compose et envoie un e-mail correctement mis en forme. Vous devez uniquement indiquer les adresses d'expédition et de destination, un objet et le corps du message. Amazon SES se charge de tout le reste. Pour plus d'informations, consultez Envoi d'e-mails formatés à l'aide de l'API Amazon SES.
- Brut – Vous composez et envoyez manuellement un e-mail, en spécifiant vos propres en-têtes d'e-mail et types MIME. Si vous avez l'habitude de mettre en forme vos e-mails, l'interface brute vous donne plus de contrôle sur la composition de votre message. Pour plus d'informations, consultez Envoi d'e-mails bruts à l'aide de l'API Amazon SES v2.

Table des matières

Envoi d'e-mails formatés à l'aide de l'API Amazon SES

Vous pouvez envoyer un e-mail formaté en utilisant AWS Management Console ou en appelant l'API Amazon SES directement via une application, ou indirectement via un AWS SDK, le AWS Command Line Interface, ou le. AWS Tools for Windows PowerShell

L'API Amazon SES fournit l'action `SendEmail`, qui vous permet de créer et d'envoyer un e-mail formaté. `SendEmail` nécessite une adresse From :, une adresse To :, un objet de message et un corps de message-texte, HTML ou les deux). Pour plus d'informations, consultez SendEmail(Référence d'API) ou SendEmail(Référence d'API v2).

> **Note**
>
> La chaîne de l'adresse e-mail doit être au format ASCII 7 bits. Si vous souhaitez effectuer un envoi vers ou à partir d'adresses e-mail qui contiennent des caractères Unicode dans la

partie domaine de l'adresse, vous devez encoder le domaine à l'aide de Punycode. Pour en savoir plus, consultez RFC 3492.

Pour obtenir des exemples sur la façon de composer un message formaté à l'aide de différents langages de programmation, consultez Exemples de code.

Pour accéder à des astuces sur la manière d'augmenter la vitesse d'envoi des e-mails lorsque vous effectuez plusieurs appels à `SendEmail`, consultez Accroissement du débit avec Amazon SES.

Envoi d'e-mails bruts à l'aide de l'API Amazon SES v2

Vous pouvez utiliser l'`SendEmail`opération Amazon SES API v2 avec le type de contenu spécifié `raw` pour envoyer des messages personnalisés à vos destinataires en utilisant le format d'e-mail brut.

À propos des champs d'en-tête d'e-mail

Le protocole SMTP (SMTP) spécifie la façon dont les e-mails doivent être envoyés en définissant l'enveloppe et certains paramètres des e-mails, mais il ne s'occupe pas du contenu du message. En revanche, le format IMF (RFC 5322) définit la manière dont le message sera composé.

Avec la spécification IMF, chaque e-mail est composé d'un en-tête et d'un corps. L'en-tête est composé des métadonnées du message et le corps contient le message lui-même. Pour en savoir plus sur les en-têtes et corps d'e-mail, consultez Format d'e-mail dans Amazon SES.

Utilisation de MIME

Le protocole SMTP a été initialement conçu pour envoyer des messages électroniques qui ne comportent que des caractères ASCII 7 bits. Cette spécification rend SMTP insuffisant pour les codages de texte non ASCII (par exemple, en Unicode), les contenus binaires ou les pièces jointes. Le standard MIME (Multipurpose Internet Mail Extensions standard) a été développé pour permettre d'envoyer beaucoup d'autres types de contenus à l'aide de SMTP.

Le standard MIME fonctionne en divisant le corps du message en plusieurs parties, puis en indiquant ce qui doit être fait avec chaque partie. Par exemple, une partie du corps de l'e-mail peut être un texte brut, tandis qu'une autre sera en HTML. En outre, le standard MIME autorise les e-mails à contenir une ou plusieurs pièces jointes. Les destinataires des messages peuvent consulter les pièces jointes depuis leurs clients de messagerie ou ils peuvent enregistrer les pièces jointes.

L'en-tête du message et le contenu sont séparés par une ligne vide. Chaque partie de l'e-mail est séparée par une limite, une chaîne de caractères qui indique le début et la fin de chaque partie.

Le message en plusieurs parties de l'exemple suivant contient un texte et une partie HTML, et une pièce jointe. La pièce jointe doit être placée juste en dessous des en-têtes de pièce jointe et est le plus souvent encodée en `base64`, comme indiqué dans cet exemple.

```
From: "Sender Name" <sender@example.com>
To: recipient@example.com
Subject: Customer service contact info
Content-Type: multipart/mixed;
    boundary="a3f166a86b56ff6c37755292d690675717ea3cd9de81228ec2b76ed4a15d6d1a"

--a3f166a86b56ff6c37755292d690675717ea3cd9de81228ec2b76ed4a15d6d1a
Content-Type: multipart/alternative;
    boundary="sub_a3f166a86b56ff6c37755292d690675717ea3cd9de81228ec2b76ed4a15d6d1a"

--sub_a3f166a86b56ff6c37755292d690675717ea3cd9de81228ec2b76ed4a15d6d1a
Content-Type: text/plain; charset=iso-8859-1
Content-Transfer-Encoding: quoted-printable

Please see the attached file for a list of customers to contact.

--sub_a3f166a86b56ff6c37755292d690675717ea3cd9de81228ec2b76ed4a15d6d1a
Content-Type: text/html; charset=iso-8859-1
Content-Transfer-Encoding: quoted-printable

<html>
<head></head>
<body>
<h1>Hello!</h1>
<p>Please see the attached file for a list of customers to contact.</p>
</body>
</html>

--sub_a3f166a86b56ff6c37755292d690675717ea3cd9de81228ec2b76ed4a15d6d1a--

--a3f166a86b56ff6c37755292d690675717ea3cd9de81228ec2b76ed4a15d6d1a
Content-Type: text/plain; name="customers.txt"
Content-Description: customers.txt
Content-Disposition: attachment;filename="customers.txt";
    creation-date="Sat, 05 Aug 2017 19:35:36 GMT";
Content-Transfer-Encoding: base64
```

```
SUQsRmlyc3ROYW1lLExhc3ROYW1lLENvdW50cnkKMzQ4LEpvaG4sU3RpbGVzLENhbmFkYQo5MjM4
OSxKaWUsTGl1LENoaW5hCjczNCxTaGlybGV5LFJvZHJpZ3VleixVbml0ZWQgU3RhdGVzCjI4OTMs
QW5heWEsSXllbmdhcixJbmRpYQ==

--a3f166a86b56ff6c37755292d690675717ea3cd9de81228ec2b76ed4a15d6d1a--
```

Le type de contenu pour le message est `multipart/mixed`, ce qui indique que le message est composé de nombreuses parties (dans cet exemple, un corps et une pièce jointe) et que le client destinataire doit gérer chaque partie séparément.

Une deuxième partie qui utilise le type de contenu `multipart/alternative` est imbriquée dans le corps. Ce type de contenu indique que chaque partie contient des versions alternatives du même contenu (dans ce cas, une version texte et une version HTML). Si le client de messagerie du destinataire peut afficher du contenu HTML, il affiche alors la version HTML du corps du message. Si le client de messagerie du destinataire ne peut pas afficher de contenu HTML, il affiche alors la version texte brut du corps du message.

Les deux versions du message contiendront également une pièce jointe (dans ce cas, un petit fichier texte qui contient des noms de client).

Lorsque vous imbriquez une partie MIME au sein d'une autre partie, comme dans cet exemple, la partie imbriquée doit utiliser un paramètre `boundary` distinct du paramètre `boundary` de la partie principale. Ces limites doivent être des chaînes de caractères uniques. Pour définir une limite entre des parties MIME, tapez deux tirets (--) suivis par la chaîne de limite. À la fin d'une partie MIME, placez deux tirets au début et à la fin de la chaîne de limite.

> **Note**
>
> Un message ne peut pas comporter plus de 500 parties MIME.

Encodage MIME

Pour maintenir la compatibilité avec des systèmes plus anciens, Amazon SES respecte la restriction ASCII 7 bits de SMTP telle que définie dans RFC 2821. Si vous souhaitez envoyer du contenu qui contient des caractères non ASCII, vous devez encoder ces caractères dans un format qui utilise des caractères ASCII 7 bits.

Adresses e-mail

La chaîne de l'adresse e-mail doit être au format ASCII 7 bits. Si vous souhaitez effectuer un envoi vers ou à partir d'adresses e-mail qui contiennent des caractères Unicode dans la partie domaine de l'adresse, vous devez encoder le domaine à l'aide de Punycode. La syntaxe Punycode n'est pas autorisée dans la partie locale de l'adresse e-mail (c'est-à-dire, la partie qui précède le signe @) ni dans le « nom d'expéditeur convivial ». Si vous souhaitez utiliser des caractères Unicode dans le « nom d'expéditeur convivial », vous devez l'encoder en employant une syntaxe de mots encodés MIME, comme indiqué dans Envoi d'e-mails bruts à l'aide de l'API Amazon SES v2. Pour en savoir plus sur Punycode, consultez RFC 3492.

> **Note**
>
> Cette règle ne s'applique qu'aux adresses e-mail que vous spécifiez dans l'enveloppe de message, non dans les en-têtes de message. Lorsque vous utilisez l'`SendEmail`opération Amazon SES API v2, les adresses que vous spécifiez dans les `Destinations` paramètres `Source` et définissent respectivement l'expéditeur et les destinataires de l'enveloppe.

En-têtes d'e-mail

Pour encoder un message d'en-tête, utilisez la syntaxe encodée MIME. La syntaxe encodée MIME utilise le format suivant :

```
=?charset?encoding?encoded-text?=
```

La valeur de *`encoding`* peut être `Q` ou `B`. Si la valeur de codage est `Q`, la valeur *`encoded-text`* doit utiliser l'encodage Q. Si la valeur de codage est `B`, la valeur de *`encoded-text`* doit utiliser l'encodage base64.

Par exemple, si vous voulez utiliser la chaîne « Як ти поживаєш? » dans la ligne d'objet d'un e-mail, vous pouvez utiliser l'un des encodages suivants :

- Encodage Q

```
=?utf-8?Q?
=D0=AF=D0=BA_=D1=82=D0=B8_=D0=BF=D0=BE=D0=B6=D0=B8=D0=B2=D0=B0=D1=94=D1=88=3F?=
```

- Encodage Base64

```
=?utf-8?B?0K/QuiDRgtC4INC/0L7QttC40LLQsNGU0Yg/?=
```

Pour en savoir plus sur l'encodage Q, consultez RFC 2047. Pour en savoir plus sur l'encodage base64, consultez RFC 2045.

Corps du message

Pour encoder le corps d'un message, vous pouvez utiliser l'encodage des guillemets imprimables ou l'encodage base64. Ensuite, utilisez l'en-tête `Content-Transfer-Encoding` pour indiquer le schéma d'encodage utilisé.

Par exemple, supposons que le corps de votre message contienne le texte suivant :

१९७२ मे रे टॉमलंसिन ने पहला ई-मेल सेंदश भेजा | रे टॉमलंसिन ने ही स्रव्परथम @ चन्हि का चयन कयिा और इनही को ईमल का आवषिकारक माना जाता है

Si vous choisissez d'encoder ce texte en utilisant l'encodage base64, commencez par spécifier l'en-tête suivant :

```
Content-Transfer-Encoding: base64
```

Ensuite, dans la section du corps de l'e-mail, incluez le texte codé en base64 :

```
4KWn4KWv4KWt4KWoIOCkruClhyDgpLDgpYcg4KSf4KWJ4KSu4KSy4KS/4KSC4KS44KSoIOCkqOCl
hyDgpKrgpLngpLLgpL4g4KSILeCkruClh+CksiDgpLjgpILgpKbgpYfgpLYg4KSt4KWH4KSc4KS+
IHwg4KSw4KWHIOCkn+ClieCkruCksuCkv+CkguCkuOCkqCDgpKjgpYcg4KS54KWAIOCkuOCksOCl
jeCkteCkquCljeCksOCkpeCkriBAIOCkmuCkv+CkqOCljeCkuSDgpJXgpL4g4KSa4KSv4KSoIOCk
leCkv+Ckr+CkviDgpJTgpLAg4KSH4KSo4KWN4KS54KWAIOCkleCliyDgpIjgpK7gpYfgpLIg4KSV
4KS+IOCkhuCkteCkteCkv+Ckt+CljeCkleCkvuCksOCklSDgpK7gpL7gpKjgpL4g4KSc4KS+4KSk
IOCkueCliCAo=
```

> **Note**
>
> Dans certains cas, vous pouvez utiliser le `Content-Transfer-Encoding` 8 bits dans les messages que vous envoyez à l'aide d'Amazon SES. Toutefois, si Amazon SES doit apporter de modifications à vos messages (par exemple, lorsque vous utilisez le suivi des ouvertures et des clics), le contenu codé en 8 bits peut ne pas s'afficher correctement quand il arrive

dans les boîtes de réception de vos destinataires. Pour cette raison, vous devez toujours encoder le contenu qui n'est pas au format ASCII 7 bits.

Attachement de fichiers

Pour attacher un fichier à un e-mail, vous devez encoder la pièce jointe à l'aide de l'encodage base64. Les pièces jointes sont généralement placées dans les parties de message MIME dédiées, qui incluent les en-têtes suivants :

- Content-Type : type de fichier de la pièce jointe. Voici des exemples de déclarations Content-Type MIME courantes :
  - Fichier en texte brut : `Content-Type: text/plain; name="sample.txt"`
  - Document Microsoft Word : `Content-Type: application/msword; name="document.docx"`
  - Image JPG : `Content-Type: image/jpeg; name="photo.jpeg"`
- Content-Disposition : spécifie la façon dont le client de messagerie du destinataire doit gérer le contenu. Pour les pièces jointes, cette valeur est `Content-Disposition: attachment`.
- Content-Transfer-Encoding : schéma ayant été utilisé pour encoder la pièce jointe. Pour les pièces jointes, cette valeur est presque toujours `base64`.
- La pièce jointe encodée : vous devez encoder la pièce jointe proprement dite et l'inclure dans le corps, sous les en-têtes de pièces jointes, comme indiqué dans l'exemple.

Amazon SES accepte la plupart des types de fichiers courants. Pour obtenir une liste des types de fichiers qu'Amazon SES n'accepte pas, reportez-vous à la section Types de pièces jointes non pris en charge par Amazon SES.

Envoi d'e-mails bruts à l'aide de l'API Amazon SES v2

L'API Amazon SES v2 fournit l'`SendEmail`action, qui vous permet de composer et d'envoyer un e-mail dans le format que vous spécifiez lorsque vous définissez le type de contenu sur simple, brut ou modélisé. Pour une description complète, voir `SendEmail`. L'exemple suivant indiquera le type de contenu à utiliser `raw` pour envoyer un message en utilisant le format d'e-mail brut.

> **Note**
>
> Pour accéder à des astuces sur la manière d'augmenter la vitesse d'envoi des e-mails lorsque vous effectuez plusieurs appels à `SendEmail`, consultez Accroissement du débit avec Amazon SES.

Le corps du message doit contenir un message brut formaté correctement, avec les champs d'en-tête et le codage de corps de message appropriés. Bien qu'il soit possible de composer le message brut manuellement au sein d'une application, il est nettement plus facile de le faire à l'aide de bibliothèques de messagerie existantes.

Java

L'exemple de code suivant montre comment utiliser la JavaMailbibliothèque et AWS SDK for Javacomment composer et envoyer un e-mail brut.

```
package com.amazonaws.samples;

import java.io.ByteArrayOutputStream;
import java.io.IOException;
import java.io.PrintStream;
import java.nio.ByteBuffer;
import java.util.Properties;

// JavaMail libraries. Download the JavaMail API
// from https://javaee.github.io/javamail/
import javax.activation.DataHandler;
import javax.activation.DataSource;
import javax.activation.FileDataSource;
import javax.mail.Message;
import javax.mail.MessagingException;
import javax.mail.Session;
import javax.mail.internet.AddressException;
import javax.mail.internet.InternetAddress;
import javax.mail.internet.MimeBodyPart;
import javax.mail.internet.MimeMessage;
import javax.mail.internet.MimeMultipart;

// AWS SDK libraries. Download the AWS SDK for Java // from https://aws.amazon.com/
sdk-for-java
import com.amazonaws.regions.Regions;
```

```
import com.amazonaws.services.simpleemail.AmazonSimpleEmailService;
import com.amazonaws.services.simpleemail.AmazonSimpleEmailServiceClientBuilder;
import com.amazonaws.services.simpleemail.model.RawMessage;
import com.amazonaws.services.simpleemail.model.SendRawEmailRequest;

public class AmazonSESSample {

 // Replace sender@example.com with your "From" address.
 // This address must be verified with Amazon SES.
 private static String SENDER = "Sender Name <sender@example.com>";

 // Replace recipient@example.com with a "To" address. If your account
 // is still in the sandbox, this address must be verified.
 private static String RECIPIENT = "recipient@example.com";

 // Specify a configuration set. If you do not want to use a configuration
 // set, comment the following variable, and the
 // ConfigurationSetName=CONFIGURATION_SET argument below.
 private static String CONFIGURATION_SET = "ConfigSet";

 // The subject line for the email.
 private static String SUBJECT = "Customer service contact info";

 // The full path to the file that will be attached to the email.
 // If you're using Windows, escape backslashes as shown in this variable.
 private static String ATTACHMENT = "C:\\Users\\sender\\customers-to-contact.xlsx";

 // The email body for recipients with non-HTML email clients.
 private static String BODY_TEXT = "Hello,\r\n"
                                   + "Please see the attached file for a list "
                                   + "of customers to contact.";

 // The HTML body of the email.
 private static String BODY_HTML = "<html>"
                                   + "<head></head>"
                                   + "<body>"
                                   + "<h1>Hello!</h1>"
                                   + "<p>Please see the attached file for a "
                                   + "list of customers to contact.</p>"
                                   + "</body>"
                                   + "</html>";

    public static void main(String[] args) throws AddressException,
 MessagingException, IOException {
```

```
    Session session = Session.getDefaultInstance(new Properties());

       // Create a new MimeMessage object.
       MimeMessage message = new MimeMessage(session);

       // Add subject, from and to lines.
       message.setSubject(SUBJECT, "UTF-8");
       message.setFrom(new InternetAddress(SENDER));
       message.setRecipients(Message.RecipientType.TO,
InternetAddress.parse(RECIPIENT));

       // Create a multipart/alternative child container.
       MimeMultipart msg_body = new MimeMultipart("alternative");

       // Create a wrapper for the HTML and text parts.
       MimeBodyPart wrap = new MimeBodyPart();

       // Define the text part.
       MimeBodyPart textPart = new MimeBodyPart();
       textPart.setContent(BODY_TEXT, "text/plain; charset=UTF-8");

       // Define the HTML part.
       MimeBodyPart htmlPart = new MimeBodyPart();
       htmlPart.setContent(BODY_HTML,"text/html; charset=UTF-8");

       // Add the text and HTML parts to the child container.
       msg_body.addBodyPart(textPart);
       msg_body.addBodyPart(htmlPart);

       // Add the child container to the wrapper object.
       wrap.setContent(msg_body);

       // Create a multipart/mixed parent container.
       MimeMultipart msg = new MimeMultipart("mixed");

       // Add the parent container to the message.
       message.setContent(msg);

       // Add the multipart/alternative part to the message.
       msg.addBodyPart(wrap);

       // Define the attachment
       MimeBodyPart att = new MimeBodyPart();
```

```
        DataSource fds = new FileDataSource(ATTACHMENT);
        att.setDataHandler(new DataHandler(fds));
        att.setFileName(fds.getName());

        // Add the attachment to the message.
        msg.addBodyPart(att);

        // Try to send the email.
        try {
            System.out.println("Attempting to send an email through Amazon SES "
                               +"using the AWS SDK for Java...");

            // Instantiate an Amazon SES client, which will make the service
            // call with the supplied AWS credentials.
            AmazonSimpleEmailService client =
                    AmazonSimpleEmailServiceClientBuilder.standard()
                    // Replace US_WEST_2 with the AWS Region you're using for
                    // Amazon SES.
                    .withRegion(Regions.US_WEST_2).build();

            // Print the raw email content on the console
            PrintStream out = System.out;
            message.writeTo(out);

            // Send the email.
            ByteArrayOutputStream outputStream = new ByteArrayOutputStream();
            message.writeTo(outputStream);
            RawMessage rawMessage =
              new RawMessage(ByteBuffer.wrap(outputStream.toByteArray()));

            SendRawEmailRequest rawEmailRequest =
              new SendRawEmailRequest(rawMessage)
                  .withConfigurationSetName(CONFIGURATION_SET);

            client.sendRawEmail(rawEmailRequest);
            System.out.println("Email sent!");
        // Display an error if something goes wrong.
        } catch (Exception ex) {
          System.out.println("Email Failed");
            System.err.println("Error message: " + ex.getMessage());
            ex.printStackTrace();
        }
    }
```

```
}
```

Python

L'exemple de code suivant montre comment utiliser les packages Python email.mime et le kit AWS SDK for Python (Boto) pour composer et envoyer un e-mail brut.

```
import os
import boto3
from botocore.exceptions import ClientError
from email.mime.multipart import MIMEMultipart
from email.mime.text import MIMEText
from email.mime.application import MIMEApplication

# Replace sender@example.com with your "From" address.
# This address must be verified with Amazon SES.
SENDER = "Sender Name <sender@example.com>"

# Replace recipient@example.com with a "To" address. If your account
# is still in the sandbox, this address must be verified.
RECIPIENT = "recipient@example.com"

# Specify a configuration set. If you do not want to use a configuration
# set, comment the following variable, and the
# ConfigurationSetName=CONFIGURATION_SET argument below.
CONFIGURATION_SET = "ConfigSet"

# If necessary, replace us-west-2 with the AWS Region you're using for Amazon SES.
AWS_REGION = "us-west-2"

# The subject line for the email.
SUBJECT = "Customer service contact info"

# The full path to the file that will be attached to the email.
ATTACHMENT = "path/to/customers-to-contact.xlsx"

# The email body for recipients with non-HTML email clients.
BODY_TEXT = "Hello,\r\nPlease see the attached file for a list of customers to
 contact."

# The HTML body of the email.
BODY_HTML = """\
<html>
```

```
<head></head>
<body>
<h1>Hello!</h1>
<p>Please see the attached file for a list of customers to contact.</p>
</body>
</html>
"""

# The character encoding for the email.
CHARSET = "utf-8"

# Create a new SES resource and specify a region.
client = boto3.client('ses',region_name=AWS_REGION)

# Create a multipart/mixed parent container.
msg = MIMEMultipart('mixed')
# Add subject, from and to lines.
msg['Subject'] = SUBJECT
msg['From'] = SENDER
msg['To'] = RECIPIENT

# Create a multipart/alternative child container.
msg_body = MIMEMultipart('alternative')

# Encode the text and HTML content and set the character encoding. This step is
# necessary if you're sending a message with characters outside the ASCII range.
textpart = MIMEText(BODY_TEXT.encode(CHARSET), 'plain', CHARSET)
htmlpart = MIMEText(BODY_HTML.encode(CHARSET), 'html', CHARSET)

# Add the text and HTML parts to the child container.
msg_body.attach(textpart)
msg_body.attach(htmlpart)

# Define the attachment part and encode it using MIMEApplication.
att = MIMEApplication(open(ATTACHMENT, 'rb').read())

# Add a header to tell the email client to treat this part as an attachment,
# and to give the attachment a name.
att.add_header('Content-
Disposition','attachment',filename=os.path.basename(ATTACHMENT))

# Attach the multipart/alternative child container to the multipart/mixed
# parent container.
msg.attach(msg_body)
```

```
# Add the attachment to the parent container.
msg.attach(att)
#print(msg)
try:
    #Provide the contents of the email.
    response = client.send_raw_email(
        Source=SENDER,
        Destinations=[
            RECIPIENT
        ],
        RawMessage={
            'Data':msg.as_string(),
        },
        ConfigurationSetName=CONFIGURATION_SET
    )
# Display an error if something goes wrong.
except ClientError as e:
    print(e.response['Error']['Message'])
else:
    print("Email sent! Message ID:"),
    print(response['MessageId'])
```

Utiliser des modèles pour envoyer des e-mails personnalisés à l'aide de l'API Amazon SES

Vous pouvez utiliser l'opération CreateTemplateAPI pour créer des modèles d'e-mail. Ces modèles incluent une ligne d'objet, ainsi que les parties texte et HTML du corps de l'e-mail. Les sections objet et corps peuvent également contenir des valeurs uniques personnalisées pour chaque destinataire.

Quelques limites et autres considérations sont à prendre en compte lors de l'utilisation de ces fonctions :

- Vous pouvez créer jusqu'à 20 000 modèles d'e-mails dans chacun d'eux Région AWS.
- Chaque modèle peut avoir une taille maximale de 500 Ko, parties texte et HTML incluses.
- Vous pouvez inclure un nombre illimité de variables de remplacement dans chaque modèle.
- Vous pouvez envoyer un e-mail à 50 destinations maximum dans chaque appel de l'opération `SendBulkTemplatedEmail`. Une destination inclut la liste des destinataires, ainsi que les destinataires en Cc et Cci. Le nombre de destinations que vous pouvez contacter en un seul appel

de l'API peut être limité par le taux maximal d'envois de votre compte. Pour plus d'informations, consultez Gestion de vos limites d'envoi Amazon SES.

Cette section contient les procédures de création de modèles d'e-mail et d'envoi d'e-mails personnalisés.

> **Note**
>
> Les procédures de cette section supposent aussi que vous avez déjà installé et configuré l' AWS CLI. Pour plus d'informations sur l'installation et la configuration du AWS CLI, consultez le guide de AWS Command Line Interface l'utilisateur.

Partie 1 : Configurer des notifications d'événements d'échec d'affichage

Si vous envoyez un e-mail qui contient un contenu de personnalisation non valide, Amazon SES peut initialement accepter le message, mais ne pourra pas le remettre. Pour cette raison, si vous prévoyez d'envoyer des e-mails personnalisés, vous devez configurer Amazon SES pour envoyer des notifications d'événement d'échec d'affichage via Amazon SNS. Lorsque vous recevez une notification d'événement d'échec d'affichage, vous pouvez identifier le message qui comportait un contenu non valide, corriger les problèmes et renvoyer le message.

La procédure décrite dans cette section est facultative, mais vivement recommandée.

Pour configurer des notifications d'événement d'échec d'affichage

1. Créer une rubrique Amazon SNS. Pour obtenir les procédures, veuillez consulter Création d'une rubrique dans le Guide du développeur Amazon Simple Notification Service.
2. Abonnez-vous à la rubrique Amazon SNS. Par exemple, si vous voulez recevoir des notifications d'événement d'échec d'affichage par e-mail, abonnez un point de terminaison de messagerie (votre adresse e-mail) à la rubrique.

   Pour obtenir des procédures, veuillez consulter Abonnement à une rubrique dans le Guide du développeur Amazon Simple Notification Service.
3. Suivez les procédures de the section called “Configuration d'une destination Amazon SNS ” pour configurer vos jeux de configuration afin de publier des notifications d'événement d'échec d'affichage dans votre rubrique Amazon SNS.

Partie 2 : Créer un modèle d'e-mail

Dans cette section, vous allez utiliser l'opération CreateTemplate API pour créer un nouveau modèle d'e-mail avec des attributs de personnalisation.

Cette procédure suppose que vous avez déjà installé et configuré l' AWS CLI. Pour plus d'informations sur l'installation et la configuration du AWS CLI, consultez le guide de AWS Command Line Interface l'utilisateur.

Pour créer le modèle

1. Dans un éditeur de texte, créez un fichier. Collez le code suivant dans le fichier.

```
{
  "Template": {
    "TemplateName": "MyTemplate",
    "SubjectPart": "Greetings, {{name}}!",
    "HtmlPart": "<h1>Hello {{name}},</h1><p>Your favorite animal is
 {{favoriteanimal}}.</p>",
    "TextPart": "Dear {{name}},\r\nYour favorite animal is {{favoriteanimal}}."
  }
}
```

   Ce code contient les propriétés suivantes :

   - TemplateName— Le nom du modèle. Lorsque vous envoyez l'e-mail, vous faites référence à ce nom.
   - SubjectPart— La ligne d'objet de l'e-mail. Cette propriété peut contenir des balises de remplacement. Celles-ci utilisent le format suivant : `{{tagname}}`. Lorsque vous envoyez l'e-mail, vous pouvez attribuer une valeur à `tagname` pour chaque destination.

     L'exemple précédent contient deux balises : `{{name}}` et `{{favoriteanimal}}`.
   - HtmlPart— Le corps HTML de l'e-mail. Cette propriété peut contenir des balises de remplacement.
   - TextPart— Le corps du texte de l'e-mail. Les destinataires dont les clients de messagerie n'affichent pas l'e-mail au format HTML voient cette version de l'e-mail. Cette propriété peut contenir des balises de remplacement.
2. Personnalisez l'exemple précédent pour l'adapter à vos besoins, puis enregistrez le fichier sous `mytemplate.json`.

3. Sur la ligne de commande, entrez la commande suivante pour créer un modèle à l'aide de l'opération d'API `CreateTemplate` :

```
aws ses create-template --cli-input-json file://mytemplate.json
```

Partie 3 : Envoi de l'e-mail personnalisé

Après avoir créé un modèle d'e-mail, vous pouvez l'utiliser pour envoyer des e-mails. Deux opérations d'API sont à votre disposition pour envoyer des e-mails à l'aide de modèles : `SendTemplatedEmail` et `SendBulkTemplatedEmail`. L'opération `SendTemplatedEmail` est utile pour envoyer un e-mail personnalisé à une seule destination (un ensemble de destinataires « To » (« À »), « Cc » et « Cci » qui recevront le même e-mail). L'opération `SendBulkTemplatedEmail` permet d'envoyer des e-mails uniques à plusieurs destinations en un seul appel de l'API Amazon SES. Cette section fournit des exemples d'utilisation du pour envoyer un e-mail AWS CLI à l'aide de ces deux opérations.

Envoi d'e-mails basés sur un modèle à une seule destination

Vous pouvez utiliser l'opération `SendTemplatedEmail` pour envoyer un e-mail à une seule destination. Toutes les destinataires de l'objet `Destination` recevront le même e-mail.

Pour envoyer un e-mail fondé sur un modèle à une seule destination

1. Dans un éditeur de texte, créez un fichier. Collez le code suivant dans le fichier.

```
{
  "Source":"Mary Major <mary.major@example.com>",
  "Template": "MyTemplate",
  "ConfigurationSetName": "ConfigSet",
  "Destination": {
    "ToAddresses": [ "alejandro.rosalez@example.com"
    ]
  },
  "TemplateData": "{ \"name\":\"Alejandro\", \"favoriteanimal\": \"alligator\" }"
}
```

   Ce code contient les propriétés suivantes :

   - Source – Adresse e-mail de l'expéditeur.

- Template – Nom du modèle à appliquer à l'e-mail.
- ConfigurationSetNom : nom du jeu de configuration à utiliser lors de l'envoi de l'e-mail.

> **Note**
>
> Nous vous recommandons d'utiliser un jeu de configurations qui est configuré pour publier les événements d'échec d'affichage dans Amazon SNS. Pour plus d'informations, consultez the section called “Partie 1 : Configurer des notifications”.

- Destination – Adresses des destinataires. Vous pouvez inclure plusieurs adresses « To », « CC » et « BCC ». Lorsque vous utilisez l'opération `SendTemplatedEmail`, tous les destinataires reçoivent le même e-mail.
- TemplateData— Chaîne JSON échappée contenant des paires clé-valeur. Les clés correspondent aux variables du modèle (par exemple, `{{name}}`). Les valeurs représentent le contenu qui remplace les variables de l'e-mail.

2. Modifiez les valeurs dans le code ci-dessus selon vos besoins, puis enregistrez le fichier sous le nom `myemail.json`.
3. Pour envoyer l'e-mail, saisissez la commande suivante sur la ligne de commande :

```
aws ses send-templated-email --cli-input-json file://myemail.json
```

Envoi d'un e-mail basé sur un modèle à plusieurs destinations

Vous pouvez utiliser l'opération `SendBulkTemplatedEmail` pour envoyer un e-mail à plusieurs destinations en un seul appel de l'API. Amazon SES envoie un e-mail unique au destinataire ou aux destinataires de chaque objet `Destination`.

Pour envoyer un e-mail fondé sur un modèle à plusieurs destinations

1. Dans un éditeur de texte, créez un fichier. Collez le code suivant dans le fichier.

```
{
  "Source":"Mary Major <mary.major@example.com>",
  "Template":"MyTemplate",
  "ConfigurationSetName": "ConfigSet",
  "Destinations":[
    {
      "Destination":{
```

```
        "ToAddresses":[
          "anaya.iyengar@example.com"
        ]
      },
      "ReplacementTemplateData":"{ \"name\":\"Anaya\", \"favoriteanimal\":
\"angelfish\" }"
    },
    {
      "Destination":{
        "ToAddresses":[
          "liu.jie@example.com"
        ]
      },
      "ReplacementTemplateData":"{ \"name\":\"Liu\", \"favoriteanimal\":\"lion\" }"
    },
    {
      "Destination":{
        "ToAddresses":[
          "shirley.rodriguez@example.com"
        ]
      },
      "ReplacementTemplateData":"{ \"name\":\"Shirley\", \"favoriteanimal\":\"shark
\" }"
    },
    {
      "Destination":{
        "ToAddresses":[
          "richard.roe@example.com"
        ]
      },
      "ReplacementTemplateData":"{}"
    }
  ],
  "DefaultTemplateData":"{ \"name\":\"friend\", \"favoriteanimal\":\"unknown\" }"
}
```

Ce code contient les propriétés suivantes :

- Source – Adresse e-mail de l'expéditeur.
- Template – Nom du modèle à appliquer à l'e-mail.
- ConfigurationSetNom : nom du jeu de configuration à utiliser lors de l'envoi de l'e-mail.

> **Note**
>
> Nous vous recommandons d'utiliser un jeu de configurations qui est configuré pour publier les événements d'échec d'affichage dans Amazon SNS. Pour plus d'informations, consultez the section called “Partie 1 : Configurer des notifications”.

- Destinations – Tableau contenant un ou plusieurs objets Destination.
  - Destination – Adresses des destinataires. Vous pouvez inclure plusieurs adresses « To », « CC » et « BCC ». Lorsque vous utilisez l'opération `SendBulkTemplatedEmail`, tous les destinataires au sein du même objet `Destination` reçoivent le même e-mail.
  - ReplacementTemplateData — Objet JSON contenant des paires clé-valeur. Les clés correspondent aux variables du modèle (par exemple, `{{name}}`). Les valeurs représentent le contenu qui remplace les variables de l'e-mail.
- DefaultTemplateData — Objet JSON contenant des paires clé-valeur. Les clés correspondent aux variables du modèle (par exemple, `{{name}}`). Les valeurs représentent le contenu qui remplace les variables de l'e-mail. Cet objet contient les données de rechange. Si un objet `Destination` contient un objet JSON vide dans la propriété `ReplacementTemplateData`, les valeurs de la propriété `DefaultTemplateData` sont utilisées.

2. Modifiez les valeurs dans le code ci-dessus selon vos besoins, puis enregistrez le fichier sous le nom `mybulkemail.json`.
3. Pour envoyer l'e-mail en masse, saisissez la commande suivante sur la ligne de commande :

```
aws ses send-bulk-templated-email --cli-input-json file://mybulkemail.json
```

Personnalisation avancée des e-mails

La fonction de modèle dans Amazon SES repose sur le système de modèles Handlebars. Vous pouvez utiliser Handlebars pour créer des modèles incluant des fonctions avancées, telles que les attributs imbriqués, l'itération sur un tableau, les instructions conditionnelles de base et la création de fichiers partiels en ligne. Cette section fournit des exemples de ces fonctions.

Handlebars inclut d'autres fonctions en plus de celles documentées dans la présente section. Pour plus d'informations, veuillez consulter Built-In Helpers (Assistants intégrés) sur handlebarsjs.com.

> **Note**
>
> SES n'échappe pas le contenu HTML lors du rendu du modèle HTML d'un message. Cela implique que si vous incluez des données saisies par l'utilisateur, par exemple à partir d'un formulaire de contact, vous devrez les échapper du côté du client.

Rubriques

Analyse des attributs imbriqués

Handlebars inclut la prise en charge des chemins imbriqués, ce qui facilite l'organisation de données client complexes, ainsi que la référence à ces données dans vos modèles d'e-mails.

Par exemple, vous pouvez organiser les données des destinataires en plusieurs catégories générales. Au sein de chacune de ces catégories, vous pouvez inclure des informations détaillées. L'exemple de code suivant illustre un exemple de cette structure pour un seul destinataire :

```
{
  "meta":{
    "userId":"51806220607"
  },
  "contact":{
    "firstName":"Anaya",
    "lastName":"Iyengar",
    "city":"Bengaluru",
    "country":"India",
    "postalCode":"560052"
  },
  "subscription":[
    {
      "interest":"Sports"
    },
    {
      "interest":"Travel"
```

```
    },
    {
      "interest":"Cooking"
    }
  ]
}
```

Dans vos modèles d'e-mails, vous pouvez vous référer aux attributs imbriqués en fournissant le nom de l'attribut parent, suivi d'un point (.) et du nom de l'attribut pour lequel vous souhaitez inclure la valeur. Par exemple, si vous utilisez la structure de données de l'exemple précédent et que vous souhaitez inclure le prénom de chaque destinataire dans le modèle d'e-mail, incluez le texte suivant dans votre modèle d'e-mail : `Hello {{contact.firstName}}!`

Handlebars peut analyser les chemins imbriqués à plusieurs niveaux de profondeur, ce qui signifie que vous avez une certaine souplesse quant à la façon de structurer les données de votre modèle.

Itération au moyen de listes

L'assistant `each` itère sur les éléments d'un tableau. Le code suivant est un exemple de modèle d'e-mail utilisant l'assistant `each` pour créer une liste détaillée des centres d'intérêt de chaque destinataire.

```
{
  "Template": {
    "TemplateName": "Preferences",
    "SubjectPart": "Subscription Preferences for {{contact.firstName}}
 {{contact.lastName}}",
    "HtmlPart": "<h1>Your Preferences</h1>
                <p>You have indicated that you are interested in receiving
                  information about the following subjects:</p>
                <ul>
                  {{#each subscription}}
                    <li>{{interest}}</li>
                  {{/each}}
                </ul>
                <p>You can change these settings at any time by visiting
                   the <a href=https://www.example.com/prefererences/i.aspx?
id={{meta.userId}}>
                   Preference Center</a>.</p>",
    "TextPart": "Your Preferences\n\nYou have indicated that you are interested in
                receiving information about the following subjects:\n
                {{#each subscription}}
```

```
                  - {{interest}}\n
                {{/each}}
                \nYou can change these settings at any time by
                visiting the Preference Center at
                https://www.example.com/prefererences/i.aspx?id={{meta.userId}}"
  }
}
```

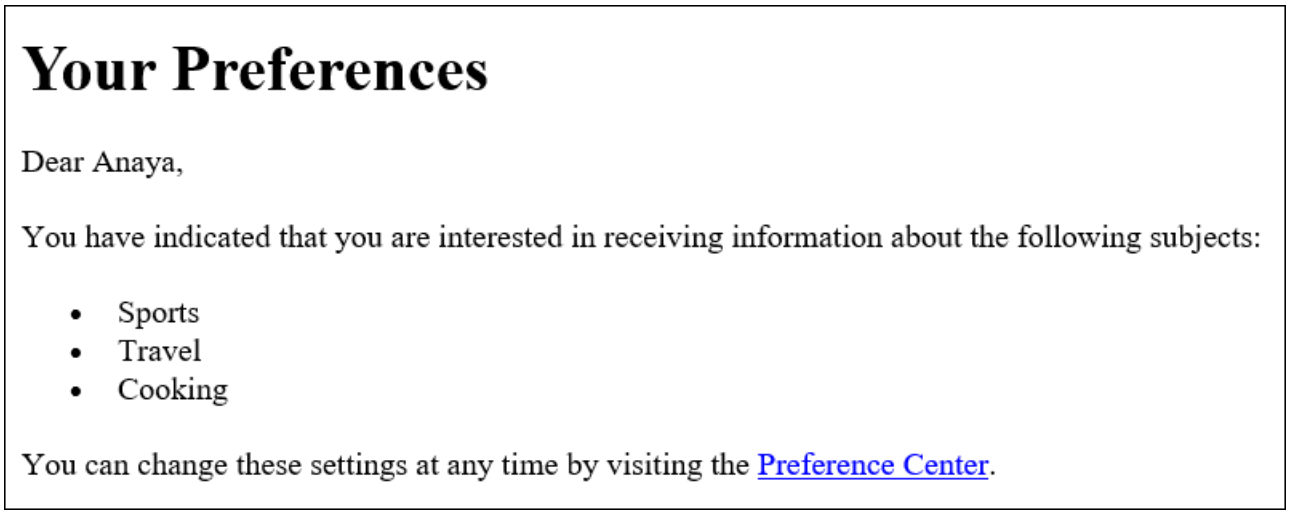
> **Important**
>
> Dans l'exemple de code précédent, les valeurs des attributs `HtmlPart` et `TextPart` comportent des sauts de ligne pour faciliter la lecture de l'exemple. Le fichier JSON de votre modèle ne peut pas contenir de sauts de ligne au sein de ces valeurs. Si vous copiez et collez cet exemple dans votre propre fichier JSON, supprimez les sauts de ligne et les espaces supplémentaires des sections `HtmlPart` et `TextPart` avant de poursuivre.

Une fois le modèle créé, vous pouvez utiliser l'opération `SendTemplatedEmail` ou `SendBulkTemplatedEmail` pour envoyer un e-mail aux destinataires à l'aide de ce modèle. Tant que chaque destinataire possède au moins une valeur dans l'objet `Interests`, il reçoit un e-mail incluant la liste détaillée de ses centres d'intérêts. L'exemple suivant illustre un fichier JSON qui peut être utilisé pour envoyer un e-mail à plusieurs destinataires à l'aide du modèle précédent :

```
{
  "Source":"Sender Name <sender@example.com>",
  "Template":"Preferences",
  "Destinations":[
    {
      "Destination":{
        "ToAddresses":[
          "anaya.iyengar@example.com"
        ]
      },
      "ReplacementTemplateData":"{\"meta\":{\"userId\":\"51806220607\"},\"contact\":
{\"firstName\":\"Anaya\",\"lastName\":\"Iyengar\"},\"subscription\":[{\"interest\":
\"Sports\"},{\"interest\":\"Travel\"},{\"interest\":\"Cooking\"}]}"
      },
    {
      "Destination":{
        "ToAddresses":[
          "shirley.rodriguez@example.com"
```

```
        ]
      },
      "ReplacementTemplateData":"{\"meta\":{\"userId\":\"1981624758263\"},\"contact\":
{\"firstName\":\"Shirley\",\"lastName\":\"Rodriguez\"},\"subscription\":[{\"interest\":
\"Technology\"},{\"interest\":\"Politics\"}]}"
    }
  ],
  "DefaultTemplateData":"{\"meta\":{\"userId\":\"\"},\"contact\":{\"firstName\":
\"Friend\",\"lastName\":\"\"},\"subscription\":[]}"
}
```

Lorsque vous envoyez un e-mail aux destinataires listés dans l'exemple précédent à l'aide de l'opération `SendBulkTemplatedEmail`, ceux-ci reçoivent un message semblable à l'exemple illustré dans l'image suivante :



Your Preferences

Dear Anaya,

You have indicated that you are interested in receiving information about the following subjects:

- Sports
- Travel
- Cooking

You can change these settings at any time by visiting the Preference Center.

Utilisation des instructions conditionnelles de base

Cette section repose sur l'exemple décrit dans la section précédente. L'exemple de la section précédente utilise l'assistant `each` pour itérer sur une liste de centres d'intérêt. Cependant, les destinataires pour lesquels aucun centre d'intérêt n'est spécifié reçoivent un e-mail avec une liste vide. À l'aide de l'assistant `{{if}}`, vous pouvez formater l'e-mail différemment si un certain attribut est présent dans les données du modèle. Le code suivant utilise l'assistant `{{if}}` pour afficher la liste à puces de la section précédente si le tableau `Subscription` contient des valeurs. Si le tableau est vide, un autre bloc de texte s'affiche.

```
{
  "Template": {
    "TemplateName": "Preferences2",
```

```
    "SubjectPart": "Subscription Preferences for {{contact.firstName}}
 {{contact.lastName}}",
    "HtmlPart": "<h1>Your Preferences</h1>
                <p>Dear {{contact.firstName}},</p>
                {{#if subscription}}
                  <p>You have indicated that you are interested in receiving
                    information about the following subjects:</p>
                    <ul>
                    {{#each subscription}}
                      <li>{{interest}}</li>
                    {{/each}}
                    </ul>
                    <p>You can change these settings at any time by visiting
                      the <a href=https://www.example.com/prefererences/i.aspx?
id={{meta.userId}}>
                      Preference Center</a>.</p>
                {{else}}
                  <p>Please update your subscription preferences by visiting
                    the <a href=https://www.example.com/prefererences/i.aspx?
id={{meta.userId}}>
                    Preference Center</a>.
                {{/if}}",
    "TextPart": "Your Preferences\n\nDear {{contact.firstName}},\n\n
                {{#if subscription}}
                  You have indicated that you are interested in receiving
                  information about the following subjects:\n
                  {{#each subscription}}
                    - {{interest}}\n
                  {{/each}}
                  \nYou can change these settings at any time by visiting the
                  Preference Center at https://www.example.com/prefererences/i.aspx?
id={{meta.userId}}.
                {{else}}
                  Please update your subscription preferences by visiting the
                  Preference Center at https://www.example.com/prefererences/i.aspx?
id={{meta.userId}}.
                {{/if}}"
  }
}
```

> **Important**
>
> Dans l'exemple de code précédent, les valeurs des attributs `HtmlPart` et `TextPart` comportent des sauts de ligne pour faciliter la lecture de l'exemple. Le fichier JSON de votre modèle ne peut pas contenir de sauts de ligne au sein de ces valeurs. Si vous copiez et collez cet exemple dans votre propre fichier JSON, supprimez les sauts de ligne et les espaces supplémentaires des sections `HtmlPart` et `TextPart` avant de poursuivre.

L'exemple suivant illustre un fichier JSON qui peut être utilisé pour envoyer un e-mail à plusieurs destinataires à l'aide du modèle précédent :

```
{
  "Source":"Sender Name <sender@example.com>",
  "Template":"Preferences2",
  "Destinations":[
    {
      "Destination":{
        "ToAddresses":[
          "anaya.iyengar@example.com"
        ]
      },
      "ReplacementTemplateData":"{\"meta\":{\"userId\":\"51806220607\"},\"contact\":
{\"firstName\":\"Anaya\",\"lastName\":\"Iyengar\"},\"subscription\":[{\"interest\":
\"Sports\"},{\"interest\":\"Cooking\"}]}"
      },
    {
      "Destination":{
        "ToAddresses":[
          "shirley.rodriguez@example.com"
        ]
      },
      "ReplacementTemplateData":"{\"meta\":{\"userId\":\"1981624758263\"},\"contact\":
{\"firstName\":\"Shirley\",\"lastName\":\"Rodriguez\"}}"
    }
  ],
  "DefaultTemplateData":"{\"meta\":{\"userId\":\"\"},\"contact\":{\"firstName\":
\"Friend\",\"lastName\":\"\"},\"subscription\":[]}"
}
```

Dans cet exemple, le destinataire dont les données du modèle incluaient une liste de centres d'intérêt reçoit le même e-mail que l'exemple de la section précédente. Le destinataire dont les données du modèle ne contenaient pas de centre d'intérêt reçoit, néanmoins, un e-mail similaire à l'exemple de l'image suivante :

Création de fichiers partiels en ligne

Vous pouvez utiliser les fichiers partiels en ligne pour simplifier les modèles incluant des répétitions de chaîne. Par exemple, il est possible de créer un fichier partiel en ligne incluant le prénom du destinataire et, s'il est disponible, son nom de famille, en ajoutant le code suivant au début de votre modèle :

```
{{#* inline \"fullName\"}}{{firstName}}{{#if lastName}} {{lastName}}{{/if}}{{/
inline}}\n
```

> **Note**
>
> Le caractère de nouvelle ligne (\n) est nécessaire pour séparer le bloc `{{inline}}` du contenu de votre modèle. Le caractère de nouvelle ligne n'apparaît pas dans la sortie finale.

Une fois que vous avez créé le fichier partiel `fullName`, vous pouvez l'inclure n'importe où dans votre modèle en faisant précéder son nom du symbole **>** (supérieur à) suivi d'un espace, comme dans l'exemple suivant : `{{> fullName}}`. Les fichiers partiels en ligne ne sont pas transférés d'une partie à l'autre de l'e-mail. Par exemple, si vous voulez utiliser le même fichier partiel dans la version HTML et la version texte de l'e-mail, vous devez le définir dans les deux sections `HtmlPart` et `TextPart`.

Vous pouvez également utiliser les fichiers partiels en ligne lors de l'itération sur les tableaux. Vous pouvez utiliser le code suivant pour créer un modèle qui recourt au fichier partiel en ligne `fullName`. Dans cet exemple, le fichier partiel en ligne s'applique à la fois au nom du destinataire et à un tableau des autres noms :

```
{
  "Template": {
    "TemplateName": "Preferences3",
    "SubjectPart": "{{firstName}}'s Subscription Preferences",
    "HtmlPart": "{{#* inline \"fullName\"}}
                  {{firstName}}{{#if lastName}} {{lastName}}{{/if}}
                {{/inline~}}\n
                <h1>Hello {{> fullName}}!</h1>
                <p>You have listed the following people as your friends:</p>
                <ul>
                {{#each friends}}
                  <li>{{> fullName}}</li>
                {{/each}}</ul>",
    "TextPart": "{{#* inline \"fullName\"}}
                  {{firstName}}{{#if lastName}} {{lastName}}{{/if}}
                {{/inline~}}\n
                Hello {{> fullName}}! You have listed the following people
                as your friends:\n
                {{#each friends}}
                  - {{> fullName}}\n
                {{/each}}"
  }
}
```

> **Important**
>
> Dans l'exemple de code précédent, les valeurs des attributs `HtmlPart` et `TextPart` comportent des sauts de ligne pour faciliter la lecture de l'exemple. Le fichier JSON de votre modèle ne peut pas contenir de sauts de ligne au sein de ces valeurs. Si vous copiez et collez cet exemple dans votre propre fichier JSON, supprimez les sauts de ligne et les espaces supplémentaires de ces sections.

Gestion des modèles d'e-mail

En plus de créer des modèles d'e-mail, vous pouvez également utiliser l'API Amazon SES pour mettre à jour ou supprimer des modèles existants, répertorier tous vos modèles existants ou afficher le contenu d'un modèle.

Cette section contient les procédures d'utilisation du AWS CLI pour effectuer des tâches liées aux modèles Amazon SES.

> **Note**
>
> Les procédures de cette section supposent aussi que vous avez déjà installé et configuré l' AWS CLI. Pour plus d'informations sur l'installation et la configuration du AWS CLI, consultez le guide de AWS Command Line Interface l'utilisateur.

Affichage d'une liste de modèles d'e-mail

Vous pouvez utiliser l'ListTemplatesopération dans l'API Amazon SES pour afficher la liste de tous vos modèles d'e-mails existants.

Pour afficher une liste de modèles d'e-mail

- Sur la ligne de commande, entrez la commande suivante :

  ```
  aws ses list-templates
  ```

  S'il existe des modèles d'e-mail existants dans votre compte Amazon SES dans la région actuelle, cette commande renvoie une réponse semblable à l'exemple suivant :

  ```
  {
      "TemplatesMetadata": [
          {
              "Name": "SpecialOffers",
              "CreatedTimestamp": "2020-08-05T16:04:12.640Z"
          },
          {
              "Name": "NewsAndUpdates",
              "CreatedTimestamp": "2019-10-03T20:03:34.574Z"
          }
      ]
  }
  ```

  Si vous n'avez pas créé de modèles, la commande renvoie un objet `TemplatesMetadata` sans membre.

Affichage du contenu d'un modèle d'e-mail spécifique

Vous pouvez utiliser l'GetTemplateopération dans l'API Amazon SES pour afficher le contenu d'un modèle d'e-mail spécifique.

Pour afficher le contenu d'un modèle d'e-mail

- Sur la ligne de commande, entrez la commande suivante :

```
aws ses get-template --template-name MyTemplate
```

  Dans la commande précédente, remplacez *MyTemplate*par le nom du modèle que vous souhaitez afficher.

  Si le nom de modèle que vous avez fourni correspond à un modèle existant dans votre compte Amazon SES, cette commande renvoie une réponse semblable à l'exemple suivant :

```
{
    "Template": {
        "TemplateName": "TestMessage",
        "SubjectPart": "Amazon SES Test Message",
        "TextPart": "Hello! This is the text part of the message.",
        "HtmlPart": "<html>\n<body>\n<h2>Hello!</h2>\n<p>This is the HTML part of
 the message.</p></body>\n</html>"
    }
}
```

  Si le nom de modèle que vous avez fourni ne correspond pas à un modèle existant dans votre compte Amazon SES, la commande renvoie une erreur `TemplateDoesNotExist`.

Suppression d'un modèle d'e-mail

Vous pouvez utiliser l'DeleteTemplateopération dans l'API Amazon SES pour supprimer un modèle d'e-mail spécifique.

Pour supprimer un modèle d'e-mail

- Sur la ligne de commande, entrez la commande suivante :

```
aws ses delete-template --template-name MyTemplate
```

Dans la commande précédente, remplacez *MyTemplate*par le nom du modèle que vous souhaitez supprimer.

Cette commande ne fournit aucune sortie. Vous pouvez vérifier que le modèle a été supprimé à l'aide de cette GetTemplateopération.

Mise à jour d'un modèle d'e-mail

Vous pouvez utiliser l'UpdateTemplateopération dans l'API Amazon SES pour mettre à jour un modèle d'e-mail existant. Par exemple, cette opération est utile si vous souhaitez modifier la ligne d'objet du modèle d'e-mail ou si vous devez modifier le corps du message lui-même.

Pour mettre à jour un modèle d'e-mail

1. Utilisez la commande `GetTemplate` pour récupérer le modèle existant en entrant la commande suivante sur la ligne de commande :

   ```
   aws ses get-template --template-name MyTemplate
   ```

   Dans la commande précédente, remplacez *MyTemplate*par le nom du modèle que vous souhaitez mettre à jour.

   Si le nom de modèle que vous avez fourni correspond à un modèle existant dans votre compte Amazon SES, cette commande renvoie une réponse semblable à l'exemple suivant :

   ```
   {
       "Template": {
           "TemplateName": "TestMessage",
           "SubjectPart": "Amazon SES Test Message",
           "TextPart": "Hello! This is the text part of the message.",
           "HtmlPart": "<html>\n<body>\n<h2>Hello!</h2>\n<p>This is the HTML part of
    the message.</p></body>\n</html>"
       }
   }
   ```

2. Dans un éditeur de texte, créez un fichier. Collez la sortie de la commande précédente dans le fichier.

3. Modifiez le modèle selon les besoins. Toutes les lignes que vous omettez sont supprimées du modèle. Par exemple, si vous souhaitez uniquement modifier le `SubjectPart` du modèle, vous devez toujours inclure les propriétés `TextPart` et `HtmlPart`.

   Lorsque vous avez terminé, enregistrez le fichier sous `update_template.json`.

4. Sur la ligne de commande, entrez la commande suivante :

   ```
   aws ses update-template --cli-input-json file://path/to/update_template.json
   ```

   Dans la commande précédente, remplacez *`path/to/update_template.json`* par le chemin d'accès au fichier `update_template.json` que vous avez créé à l'étape précédente.

   Si le modèle est mis à jour avec succès, cette commande ne fournit aucune sortie. Vous pouvez vérifier que le modèle a été mis à jour à l'aide de cette GetTemplateopération.

   Si le modèle que vous avez spécifié n'existe pas, cette commande renvoie une erreur `TemplateDoesNotExist`. Si le modèle ne contient pas la propriété `TextPart` ou `HtmlPart` (ou les deux), cette commande renvoie une erreur `InvalidParameterValue`.

Envoi d'e-mails via Amazon SES à l'aide d'un AWS SDK

Vous pouvez utiliser un AWS SDK pour envoyer des e-mails via Amazon SES. AWS Les SDK sont disponibles pour plusieurs langages de programmation. Pour plus d'informations, veuillez consulter Outils pour Amazon Web Services.

Prérequis

Les conditions préalables suivantes doivent être remplies pour compléter l'un des exemples de code de la section suivante :

- Si vous ne l'avez pas déjà fait, suivez les étapes dans Configuration d'Amazon Simple Email Service.
- Vérifiez votre adresse e-mail avec Amazon SES – Avant de pouvoir envoyer un e-mail à l'aide d'Amazon SES, vous devez vérifier que vous êtes propriétaire de l'adresse e-mail de l'expéditeur. Si votre compte est encore dans l'environnement de test (sandbox) Amazon SES, vous devez également vérifier l'adresse e-mail du destinataire. Nous vous recommandons d'utiliser la console Amazon SES pour vérifier les adresses e-mail. Pour plus d’informations, consultez Création d'une identité d'adresse e-mail.

- Obtenez vos AWS informations d'identification —Vous avez besoin d'un identifiant de clé d' AWS accès et d'une clé d'accès AWS secrète pour accéder à Amazon SES à l'aide d'un SDK. Vous pouvez trouver vos informations d'identification via la page Informations d'identification de sécurité de la AWS Management Console. Pour en savoir plus sur les informations d'identification, consultez Types d'informations d'identification Amazon SES.
- Création d'un fichier d'informations d'identification partagé – Pour que l'exemple de code fourni dans cette section fonctionne correctement, vous devez créer un fichier d'informations d'identification partagé. Pour plus d'informations, consultez Création d'un fichier d'informations d'identification partagé à utiliser lors de l'envoi d'e-mails via Amazon SES à l'aide d'un AWS SDK.

Exemples de code

> **Important**
>
> Dans les didacticiels suivants, vous vous envoyez un e-mail afin de vérifier si vous l'avez reçu. Pour d'autres essais ou pour des tests de charge, utilisez le simulateur de boîte aux lettres Amazon SES. Les e-mails envoyés au simulateur de boîte aux lettres ne sont pas pris en compte dans votre quota d'envoi et vos taux de retours à l'expéditeur et de réclamations. Pour plus d'informations, consultez Utilisation manuelle du simulateur de boîte aux lettres.

.NET

La procédure suivante montre comment envoyer un e-mail via Amazon SES à l'aide de Visual Studio et du AWS SDK for .NET.

Cette solution a été testée en utilisant les éléments suivants :

- Microsoft Visual Studio Community 2017, version 15.4.0.
- Microsoft .NET Framework version 4.6.1.
- Le package AWSSDK .Core (version 3.3.19), installé à l'aide de. NuGet
- Le AWSSDK. SimpleEmail package (version 3.3.6.1), installé à l'aide de. NuGet

Avant de commencer, exécutez les tâches suivantes :

- Installation de Visual Studio – Visual Studio est disponible à l'adresse https://www.visualstudio.com/.

Pour envoyer un e-mail à l'aide du AWS SDK for .NET

1. Créez un projet en procédant comme suit :

   a. Démarrez Visual Studio 2015.

   b. Dans le menu File (Fichier), choisissez New (Nouveau), Project (Projet).

   c. Dans la fenêtre New Project (Nouveau projet), dans le panneau de gauche, développez Installed (Installations), puis Visual C#.

   d. Dans le panneau de droite, choisissez Console App (.NET Framework).

   e. Pour Name (Nom), tapez **`AmazonSESSample`**, puis choisissez OK.

2. NuGet À utiliser pour inclure les packages Amazon SES dans votre solution en effectuant les étapes suivantes :

   a. Dans le volet Explorateur de solutions, cliquez avec le bouton droit sur votre projet, puis sélectionnez Gérer les NuGet packages.

   b. Dans l'onglet NuGet: AmazonSessAmple, choisissez Parcourir.

   c. Dans la zone de recherche, saisissez **`AWSSDK.SimpleEmail`**.

   d. Choisissez le AWSSDK. SimpleEmailpackage, puis choisissez Installer.

   e. Dans la fenêtre Preview Changes (Prévisualiser les modifications), choisissez OK.

3. Sous l'onglet Program.cs, collez le code suivant :

```
using Amazon;
using System;
using System.Collections.Generic;
using Amazon.SimpleEmail;
using Amazon.SimpleEmail.Model;

namespace AmazonSESSample
{
    class Program
    {
        // Replace sender@example.com with your "From" address.
        // This address must be verified with Amazon SES.
        static readonly string senderAddress = "sender@example.com";

        // Replace recipient@example.com with a "To" address. If your account
        // is still in the sandbox, this address must be verified.
        static readonly string receiverAddress = "recipient@example.com";
```

```
        // The configuration set to use for this email. If you do not want to
 use a
        // configuration set, comment out the following property and the
        // ConfigurationSetName = configSet argument below.
        static readonly string configSet = "ConfigSet";

        // The subject line for the email.
        static readonly string subject = "Amazon SES test (AWS SDK for .NET)";

        // The email body for recipients with non-HTML email clients.
        static readonly string textBody = "Amazon SES Test (.NET)\r\n"
                                        + "This email was sent through Amazon
 SES "
                                        + "using the AWS SDK for .NET.";

        // The HTML body of the email.
        static readonly string htmlBody = @"<html>
<head></head>
<body>
  <h1>Amazon SES Test (AWS SDK for .NET)</h1>
  <p>This email was sent with
    <a href='https://aws.amazon.com/ses/'>Amazon SES</a> using the
    <a href='https://aws.amazon.com/sdk-for-net/'> AWS SDK for .NET</a>.</p>
</body>
</html>";

        static void Main(string[] args)
        {
            // Replace USWest2 with the AWS Region you're using for Amazon SES.
            // Acceptable values are EUWest1, USEast1, and USWest2.
            using (var client = new
 AmazonSimpleEmailServiceClient(RegionEndpoint.USWest2))
            {
                var sendRequest = new SendEmailRequest
                {
                    Source = senderAddress,
                    Destination = new Destination
                    {
                        ToAddresses =
                        new List<string> { receiverAddress }
                    },
                    Message = new Message
                    {
```

```
                        Subject = new Content(subject),
                        Body = new Body
                        {
                            Html = new Content
                            {
                                Charset = "UTF-8",
                                Data = htmlBody
                            },
                            Text = new Content
                            {
                                Charset = "UTF-8",
                                Data = textBody
                            }
                        }
                    },
                    // If you are not using a configuration set, comment
                    // or remove the following line
                    ConfigurationSetName = configSet
                };
                try
                {
                    Console.WriteLine("Sending email using Amazon SES...");
                    var response = client.SendEmail(sendRequest);
                    Console.WriteLine("The email was sent successfully.");
                }
                catch (Exception ex)
                {
                    Console.WriteLine("The email was not sent.");
                    Console.WriteLine("Error message: " + ex.Message);

                }
            }

            Console.Write("Press any key to continue...");
            Console.ReadKey();
        }
    }
}
```

4. Dans l'éditeur de code, procédez comme suit :

   - Remplacez *sender@example.com* par l'adresse e-mail « From: » (De :). Cette adresse doit être vérifiée. Pour plus d'informations, consultez Identités vérifiées.

- Remplacez *recipient@example.com* par l'adresse « To: » (À :). Si votre compte est encore dans l'environnement de test (sandbox), cette adresse doit également être vérifiée.
- Remplacez *ConfigSet*par le nom du jeu de configuration à utiliser lors de l'envoi de cet e-mail.
- Remplacez *USWest2* par le nom du point de Région AWS terminaison que vous utilisez pour envoyer des e-mails via Amazon SES. Pour connaître la liste des régions dans lesquelles Amazon SES est disponible, consultez Amazon Simple Email Service (Amazon SES) dans le document Références générales AWS.

Lorsque vous avez terminé, enregistrez `Program.cs`.

5. Concevez et exécutez l'application en effectuant les étapes suivantes :

   a. Dans le menu Build (Créer), choisissez Build Solution (Créer une solution).

   b. Dans le menu Débogage, choisissez Démarrer le débogage. Une fenêtre de la console s'affiche.

6. Vérifiez la sortie de la console. Si l'envoi de l'e-mail aboutit, la console affiche « `The email was sent successfully.` »
7. Si l'e-mail a été envoyé avec succès, connectez-vous au client de messagerie de l'adresse du destinataire. Vous verrez le message que vous avez envoyé.

Java

La procédure suivante explique comment utiliser Eclipse IDE pour les développeurs Java EE, AWS Toolkit for Eclipsecréer un projet AWS SDK et modifier le code Java pour envoyer un e-mail via Amazon SES.

Avant de commencer, exécutez les tâches suivantes :

- Installer Eclipse – Eclipse est disponible à l'adresse https://www.eclipse.org/downloads. Le code présenté dans ce didacticiel a été testé avec Eclipse Neon.3 (version 4.6.3) et la version 1.8 de l'environnement d'exécution Java.
- Installez le AWS Toolkit for Eclipse—Les instructions pour ajouter le AWS Toolkit for Eclipse à votre installation Eclipse sont disponibles sur https://aws.amazon.com/eclipse. Le code inclus dans ce didacticiel a été testé avec la version 2.3.1 du kit AWS Toolkit for Eclipse.

Pour envoyer un e-mail à l'aide du AWS SDK for Java

1. Créez un projet AWS Java dans Eclipse en effectuant les étapes suivantes :

   a. Démarrez Eclipse.

   b. Dans le menu File (Fichier), sélectionnez New (Nouveau), puis Other (Autre). Dans la fenêtre New (Nouveau), développez le dossier AWS, puis choisissez AWS Java Project (Projet Java AWS).

   c. Dans la boîte de dialogue Nouveau projet AWS Java, procédez comme suit :

      i. Pour Project name (Nom du projet), tapez un nom de projet.

      ii. Sous AWS SDK for Java Exemples, sélectionnez Amazon Simple Email Service JavaMail Sample.

      iii. Choisissez Finish (Terminer).

2. Dans le panneau Package Explorer (Explorateur de paquets) d'Eclipse, développez votre projet.

3. Sous votre projet, développez le dossier `src/main/java`, développez le dossier `com.amazon.aws.samples`, puis cliquez deux fois sur `AmazonSESSample.java`.

4. Remplacez la totalité du contenu de `AmazonSESSample.java` par le code suivant :

```
package com.amazonaws.samples;

import java.io.IOException;

import com.amazonaws.regions.Regions;
import com.amazonaws.services.simpleemail.AmazonSimpleEmailService;
import com.amazonaws.services.simpleemail.AmazonSimpleEmailServiceClientBuilder;
import com.amazonaws.services.simpleemail.model.Body;
import com.amazonaws.services.simpleemail.model.Content;
import com.amazonaws.services.simpleemail.model.Destination;
import com.amazonaws.services.simpleemail.model.Message;
import com.amazonaws.services.simpleemail.model.SendEmailRequest;

public class AmazonSESSample {

  // Replace sender@example.com with your "From" address.
  // This address must be verified with Amazon SES.
  static final String FROM = "sender@example.com";
```

```
  // Replace recipient@example.com with a "To" address. If your account
  // is still in the sandbox, this address must be verified.
  static final String TO = "recipient@example.com";

  // The configuration set to use for this email. If you do not want to use a
  // configuration set, comment the following variable and the
  // .withConfigurationSetName(CONFIGSET); argument below.
  static final String CONFIGSET = "ConfigSet";

  // The subject line for the email.
  static final String SUBJECT = "Amazon SES test (AWS SDK for Java)";

  // The HTML body for the email.
  static final String HTMLBODY = "<h1>Amazon SES test (AWS SDK for Java)</h1>"
      + "<p>This email was sent with <a href='https://aws.amazon.com/ses/'>"
      + "Amazon SES</a> using the <a href='https://aws.amazon.com/sdk-for-
java/'>"
      + "AWS SDK for Java</a>";

  // The email body for recipients with non-HTML email clients.
  static final String TEXTBODY = "This email was sent through Amazon SES "
      + "using the AWS SDK for Java.";

  public static void main(String[] args) throws IOException {

    try {
      AmazonSimpleEmailService client =
          AmazonSimpleEmailServiceClientBuilder.standard()
          // Replace US_WEST_2 with the AWS Region you're using for
          // Amazon SES.
            .withRegion(Regions.US_WEST_2).build();
      SendEmailRequest request = new SendEmailRequest()
          .withDestination(
              new Destination().withToAddresses(TO))
          .withMessage(new Message()
              .withBody(new Body()
                  .withHtml(new Content()
                      .withCharset("UTF-8").withData(HTMLBODY))
                  .withText(new Content()
                      .withCharset("UTF-8").withData(TEXTBODY)))
              .withSubject(new Content()
                  .withCharset("UTF-8").withData(SUBJECT)))
          .withSource(FROM)
          // Comment or remove the next line if you are not using a
```

```
            // configuration set
            .withConfigurationSetName(CONFIGSET);
        client.sendEmail(request);
        System.out.println("Email sent!");
      } catch (Exception ex) {
        System.out.println("The email was not sent. Error message: "
            + ex.getMessage());
      }
    }
}
```

5. Dans `AmazonSESSample.java`, remplacez les éléments suivants par vos propres valeurs :

> **Important**
>
> Les adresses e-mail sont sensibles à la casse. Assurez-vous que les adresses sont exactement les mêmes que celles que vous avez vérifiées.

- `SENDER@EXAMPLE.COM` – Remplacez par votre adresse e-mail « From ». Vous devez vérifier cette adresse avant d'exécuter ce programme. Pour plus d'informations, consultez Identités vérifiées dans Amazon SES.
- `RECIPIENT@EXAMPLE.COM` – Remplacez par votre adresse e-mail « To ». Si votre compte est encore dans l'environnement de test (sandbox), vous devez vérifier cette adresse avant de l'utiliser. Pour plus d'informations, consultez Demande d'accès à la production (sortie du sandbox d'Amazon SES).
- (Facultatif) **`us-west-2`** – Si vous souhaitez utiliser Amazon SES dans une région autre que USA Ouest (Oregon), remplacez ceci par la région que vous souhaitez utiliser. Pour connaître la liste des régions dans lesquelles Amazon SES est disponible, consultez Amazon Simple Email Service (Amazon SES) dans le document Références générales AWS.

6. Enregistrez `AmazonSESSample.java`.
7. Pour créer le projet, choisissez Project (Projet), puis Build Project (Créer un projet).

> **Note**
>
> Si cette option est désactivée, la génération automatique est peut-être activée. Dans ce cas, ignorez cette étape.

8. Pour démarrer le programme et envoyer l'e-mail, choisissez Run (Exécuter), puis à nouveau Run (Exécuter).
9. Vérifiez la sortie du panneau de la console dans Eclipse. Si l'envoi de l'e-mail aboutit, la console affiche «`Email sent!`». Dans le cas contraire, elle affiche un message d'erreur.
10. Si l'e-mail a été envoyé avec succès, connectez-vous au client de messagerie de l'adresse du destinataire. Vous verrez le message que vous avez envoyé.

PHP

Cette rubrique montre comment utiliser AWS SDK for PHP pour envoyer un e-mail via Amazon SES.

Avant de commencer, exécutez les tâches suivantes :

- Installer PHP – PHP est disponible à l'adresse http://php.net/downloads.php. Ce didacticiel nécessite PHP version 5.5 ou ultérieure. Après avoir installé PHP, ajoutez le chemin d'accès à PHP dans vos variables d'environnement afin de pouvoir exécuter PHP à partir de n'importe quelle invite de commande. Le code inclus dans ce didacticiel a été testé avec PHP 7.2.7.
- Installez la AWS SDK for PHP version 3 —Pour les instructions de téléchargement et d'installation, consultez la AWS SDK for PHP documentation. Le code inclus dans ce didacticiel a été testé avec la version 3.64.13 du kit SDK.

Pour envoyer un e-mail via Amazon SES à l'aide du AWS SDK for PHP

1. Dans un éditeur de texte, créez un fichier nommé `amazon-ses-sample.php`. Collez le code suivant :

```
<?php

// If necessary, modify the path in the require statement below to refer to the
// location of your Composer autoload.php file.
require 'vendor/autoload.php';

use Aws\Ses\SesClient;
use Aws\Exception\AwsException;

// Create an SesClient. Change the value of the region parameter if you're
// using an AWS Region other than US West (Oregon). Change the value of the
// profile parameter if you want to use a profile in your credentials file
```

```
// other than the default.
$SesClient = new SesClient([
    'profile' => 'default',
    'version' => '2010-12-01',
    'region'  => 'us-west-2'
]);

// Replace sender@example.com with your "From" address.
// This address must be verified with Amazon SES.
$sender_email = 'sender@example.com';

// Replace these sample addresses with the addresses of your recipients. If
// your account is still in the sandbox, these addresses must be verified.
$recipient_emails = ['recipient1@example.com','recipient2@example.com'];

// Specify a configuration set. If you do not want to use a configuration
// set, comment the following variable, and the
// 'ConfigurationSetName' => $configuration_set argument below.
$configuration_set = 'ConfigSet';

$subject = 'Amazon SES test (AWS SDK for PHP)';
$plaintext_body = 'This email was sent with Amazon SES using the AWS SDK for
 PHP.' ;
$html_body =  '<h1>AWS Amazon Simple Email Service Test Email</h1>'.
              '<p>This email was sent with <a href="https://aws.amazon.com/
ses/">'.
              'Amazon SES</a> using the <a href="https://aws.amazon.com/sdk-for-
php/">'.
              'AWS SDK for PHP</a>.</p>';
$char_set = 'UTF-8';

try {
    $result = $SesClient->sendEmail([
        'Destination' => [
            'ToAddresses' => $recipient_emails,
        ],
        'ReplyToAddresses' => [$sender_email],
        'Source' => $sender_email,
        'Message' => [
          'Body' => [
              'Html' => [
                  'Charset' => $char_set,
                  'Data' => $html_body,
              ],
```

```
                'Text' => [
                    'Charset' => $char_set,
                    'Data' => $plaintext_body,
                ],
            ],
            'Subject' => [
                'Charset' => $char_set,
                'Data' => $subject,
            ],
        ],
        // If you aren't using a configuration set, comment or delete the
        // following line
        'ConfigurationSetName' => $configuration_set,
    ]);
    $messageId = $result['MessageId'];
    echo("Email sent! Message ID: $messageId"."\n");
} catch (AwsException $e) {
    // output error message if fails
    echo $e->getMessage();
    echo("The email was not sent. Error message: ".$e-
>getAwsErrorMessage()."\n");
    echo "\n";
}
```

2. Dans `amazon-ses-sample.php`, remplacez les éléments suivants par vos propres valeurs :

   - **`path_to_sdk_inclusion`**—Remplacez par le chemin requis pour l'inclure AWS SDK for PHP dans le programme. Pour en savoir plus, consultez la documentation AWS SDK for PHP.
   - **`sender@example.com`** – Remplacez par une adresse e-mail que vous avez vérifiée avec Amazon SES. Pour plus d'informations, consultez Identités vérifiées. Les adresses e-mail d'Amazon SES sont sensibles à la casse. Assurez-vous que l'adresse que vous saisissez est exactement la même que celle que vous avez vérifiée.
   - **`recipient1@example.com`**, **`recipient2@example.com`** – Remplacez par les adresses des destinataires. Si votre compte est encore dans l'environnement de test (sandbox), les adresses de destination doivent également être vérifiées. Pour plus d'informations, consultez Demande d'accès à la production (sortie du sandbox d'Amazon SES). Assurez-vous que l'adresse que vous saisissez est exactement la même que celle que vous avez vérifiée.

- (Facultatif) **`ConfigSet`**– Si vous souhaitez utiliser un jeu de configurations lors de l'envoi de cet e-mail, remplacez cette valeur par le nom du jeu de configurations. Pour en savoir plus sur les jeux de configuration, consultez Utilisation des jeux de configuration dans Amazon SES.
- (Facultatif) **`us-west-2`** — Si vous souhaitez utiliser Amazon SES dans une région autre que USA Ouest (Oregon), remplacez ceci par la région que vous souhaitez utiliser. Pour connaître la liste des régions dans lesquelles Amazon SES est disponible, consultez Amazon Simple Email Service (Amazon SES) dans le document Références générales AWS.

3. Enregistrez `amazon-ses-sample.php`.
4. Pour exécuter le programme, ouvrez une invite de commande dans le même répertoire que `amazon-ses-sample.php`, puis entrez la commande suivante :

```
$ php amazon-ses-sample.php
```

5. Vérifiez la sortie. Si l'envoi de l'e-mail aboutit, la console affiche «`Email sent!`». Dans le cas contraire, elle affiche un message d'erreur.

> **Note**
>
> Si une erreur « cURL error 60: SSL certificate problem » se produit lorsque vous exécutez le programme, téléchargez la dernière solution groupée d'autorité de certification (CA), comme décrit dans la documentation AWS SDK for PHP. Ensuite, dans `amazon-ses-sample.php`, ajoutez les lignes suivantes dans le tableau `SesClient::factory`, remplacez `path_of_certs` par le chemin d'accès à la solution groupée d'autorité de certification (CA) téléchargé, et exécutez à nouveau le programme.
>
> ```
> 'http' => [
>    'verify' => 'path_of_certs\ca-bundle.crt'
> ]
> ```

6. Connectez-vous au client de messagerie de l'adresse du destinataire. Vous verrez le message que vous avez envoyé.

Ruby

Cette rubrique montre comment utiliser AWS SDK for Ruby pour envoyer un e-mail via Amazon SES.

Avant de commencer, exécutez les tâches suivantes :

- Installer Ruby – Ruby est disponible à l'adresse https://www.ruby-lang.org/en/downloads/. Le code inclus dans ce didacticiel a été testé avec Ruby 1.9.3. Après avoir installé Ruby, ajoutez le chemin d'accès à Ruby dans vos variables d'environnement afin de pouvoir exécuter Ruby à partir de n'importe quelle invite de commande.
- Installez le AWS SDK for Ruby —Pour obtenir des instructions de téléchargement et d'installation, consultez la section Installation du AWS SDK for Ruby dans le guide du AWS SDK for Ruby développeur. L'exemple de code inclus dans ce didacticiel a été testé avec la version 2.9.36 du kit AWS SDK for Ruby.
- Création d'un fichier d'informations d'identification partagé – Pour que l'exemple de code fourni dans cette section fonctionne correctement, vous devez créer un fichier d'informations d'identification partagé. Pour plus d'informations, consultez Création d'un fichier d'informations d'identification partagé à utiliser lors de l'envoi d'e-mails via Amazon SES à l'aide d'un AWS SDK.

Pour envoyer un e-mail via Amazon SES à l'aide du AWS SDK for Ruby

1. Dans un éditeur de texte, créez un fichier nommé `amazon-ses-sample.rb`. Collez le code suivant dans le fichier :

```
require 'aws-sdk'

# Replace sender@example.com with your "From" address.
# This address must be verified with Amazon SES.
sender = "sender@example.com"

# Replace recipient@example.com with a "To" address. If your account
# is still in the sandbox, this address must be verified.
recipient = "recipient@example.com"

# Specify a configuration set. If you do not want to use a configuration
# set, comment the following variable and the
# configuration_set_name: configsetname argument below.
configsetname = "ConfigSet"
```

```
# Replace us-west-2 with the AWS Region you're using for Amazon SES.
awsregion = "us-west-2"

# The subject line for the email.
subject = "Amazon SES test (AWS SDK for Ruby)"

# The HTML body of the email.
htmlbody =
  '<h1>Amazon SES test (AWS SDK for Ruby)</h1>'\
  '<p>This email was sent with <a href="https://aws.amazon.com/ses/">'\
  'Amazon SES</a> using the <a href="https://aws.amazon.com/sdk-for-ruby/">'\
  'AWS SDK for Ruby</a>.'

# The email body for recipients with non-HTML email clients.
textbody = "This email was sent with Amazon SES using the AWS SDK for Ruby."

# Specify the text encoding scheme.
encoding = "UTF-8"

# Create a new SES resource and specify a region
ses = Aws::SES::Client.new(region: awsregion)

# Try to send the email.
begin

  # Provide the contents of the email.
  resp = ses.send_email({
    destination: {
      to_addresses: [
        recipient,
      ],
    },
    message: {
      body: {
        html: {
          charset: encoding,
          data: htmlbody,
        },
        text: {
          charset: encoding,
          data: textbody,
        },
      },
```

```
      subject: {
        charset: encoding,
        data: subject,
      },
    },
  source: sender,
  # Comment or remove the following line if you are not using
  # a configuration set
  configuration_set_name: configsetname,
  })
  puts "Email sent!"

# If something goes wrong, display an error message.
rescue Aws::SES::Errors::ServiceError => error
  puts "Email not sent. Error message: #{error}"

end
```

2. Dans `amazon-ses-sample.rb`, remplacez les éléments suivants par vos propres valeurs :

   - **`sender@example.com`** – Remplacez par une adresse e-mail que vous avez vérifiée avec Amazon SES. Pour plus d'informations, consultez Identités vérifiées. Les adresses e-mail d'Amazon SES sont sensibles à la casse. Assurez-vous que l'adresse que vous saisissez est exactement la même que celle que vous avez vérifiée.
   - **`recipient@example.com`**—Remplacez par l'adresse du destinataire. Si votre compte est encore dans l'environnement de test (sandbox), vous devez vérifier cette adresse avant de l'utiliser. Pour plus d'informations, consultez Demande d'accès à la production (sortie du sandbox d'Amazon SES). Assurez-vous que l'adresse que vous saisissez est exactement la même que celle que vous avez vérifiée.
   - (Facultatif) **`us-west-2`** — Si vous souhaitez utiliser Amazon SES dans une région autre que USA Ouest (Oregon), remplacez ceci par la région que vous souhaitez utiliser. Pour connaître la liste des régions dans lesquelles Amazon SES est disponible, consultez Amazon Simple Email Service (Amazon SES) dans le document Références générales AWS.

3. Enregistrez `amazon-ses-sample.rb`.
4. Pour exécuter le programme, ouvrez une invite de commande dans le même répertoire que `amazon-ses-sample.rb`, puis entrez ruby amazon-ses-sample.rb
5. Vérifiez la sortie. Si l'envoi de l'e-mail aboutit, la console affiche «`Email sent!`». Dans le cas contraire, elle affiche un message d'erreur.

6. Connectez-vous au client de messagerie de l'adresse du destinataire. Vous trouverez le message que vous avez envoyé.

Python

Cette rubrique montre comment utiliser AWS SDK for Python (Boto) pour envoyer un e-mail via Amazon SES.

Avant de commencer, exécutez les tâches suivantes :

- Vérifiez votre adresse e-mail avec Amazon SES – Avant de pouvoir envoyer un e-mail à l'aide d'Amazon SES, vous devez vérifier que vous êtes propriétaire de l'adresse e-mail de l'expéditeur. Si votre compte est encore dans l'environnement de test (sandbox) Amazon SES, vous devez également vérifier l'adresse e-mail du destinataire. Nous vous recommandons d'utiliser la console Amazon SES pour vérifier les adresses e-mail. Pour plus d'informations, consultez Création d'une identité d'adresse e-mail.
- Obtenez vos AWS informations d'identification —Vous avez besoin d'un identifiant de clé d' AWS accès et d'une clé d'accès AWS secrète pour accéder à Amazon SES à l'aide d'un SDK. Vous pouvez trouver vos informations d'identification via la page Informations d'identification de sécurité de la AWS Management Console. Pour en savoir plus sur les informations d'identification, consultez Types d'informations d'identification Amazon SES.
- Installer Python – Python est disponible à l'adresse https://www.python.org/downloads/. Le code inclus dans ce didacticiel a été testé avec Python 2.7.6 et Python 3.6.1. Après avoir installé Python, ajoutez le chemin d'accès à Python dans vos variables d'environnement afin de pouvoir exécuter Python à partir de n'importe quelle invite de commande.
- Installez le AWS SDK for Python (Boto) —Pour obtenir des instructions de téléchargement et d'installation, consultez la AWS SDK for Python (Boto) documentation. L'exemple de code inclus dans ce didacticiel a été testé avec la version 1.4.4 du kit SDK pour Python.

Pour envoyer un e-mail via Amazon SES à l'aide du kit SDK pour Python

1. Dans un éditeur de texte, créez un fichier nommé `amazon-ses-sample.py`. Collez le code suivant dans le fichier :

```
import boto3
from botocore.exceptions import ClientError
```

```
# Replace sender@example.com with your "From" address.
# This address must be verified with Amazon SES.
SENDER = "Sender Name <sender@example.com>"

# Replace recipient@example.com with a "To" address. If your account
# is still in the sandbox, this address must be verified.
RECIPIENT = "recipient@example.com"

# Specify a configuration set. If you do not want to use a configuration
# set, comment the following variable, and the
# ConfigurationSetName=CONFIGURATION_SET argument below.
CONFIGURATION_SET = "ConfigSet"

# If necessary, replace us-west-2 with the AWS Region you're using for Amazon
 SES.
AWS_REGION = "us-west-2"

# The subject line for the email.
SUBJECT = "Amazon SES Test (SDK for Python)"

# The email body for recipients with non-HTML email clients.
BODY_TEXT = ("Amazon SES Test (Python)\r\n"
             "This email was sent with Amazon SES using the "
             "AWS SDK for Python (Boto)."
            )

# The HTML body of the email.
BODY_HTML = """<html>
<head></head>
<body>
  <h1>Amazon SES Test (SDK for Python)</h1>
  <p>This email was sent with
    <a href='https://aws.amazon.com/ses/'>Amazon SES</a> using the
    <a href='https://aws.amazon.com/sdk-for-python/'> AWS SDK for Python
 (Boto)</a>.</p>
</body>
</html>
            """

# The character encoding for the email.
CHARSET = "UTF-8"

# Create a new SES resource and specify a region.
client = boto3.client('ses',region_name=AWS_REGION)
```

```
# Try to send the email.
try:
    #Provide the contents of the email.
    response = client.send_email(
        Destination={
            'ToAddresses': [
                RECIPIENT,
            ],
        },
        Message={
            'Body': {
                'Html': {
                    'Charset': CHARSET,
                    'Data': BODY_HTML,
                },
                'Text': {
                    'Charset': CHARSET,
                    'Data': BODY_TEXT,
                },
            },
            'Subject': {
                'Charset': CHARSET,
                'Data': SUBJECT,
            },
        },
        Source=SENDER,
        # If you are not using a configuration set, comment or delete the
        # following line
        ConfigurationSetName=CONFIGURATION_SET,
    )
# Display an error if something goes wrong.
except ClientError as e:
    print(e.response['Error']['Message'])
else:
    print("Email sent! Message ID:"),
    print(response['MessageId'])
```

2. Dans `amazon-ses-sample.py`, remplacez les éléments suivants par vos propres valeurs :

   - **`sender@example.com`** – Remplacez par une adresse e-mail que vous avez vérifiée avec Amazon SES. Pour plus d'informations, consultez Identités vérifiées. Les adresses e-mail

d'Amazon SES sont sensibles à la casse. Assurez-vous que l'adresse que vous saisissez est exactement la même que celle que vous avez vérifiée.

- **`recipient@example.com`**—Remplacez par l'adresse du destinataire. Si votre compte est encore dans l'environnement de test (sandbox), vous devez vérifier cette adresse avant de l'utiliser. Pour plus d'informations, consultez Demande d'accès à la production (sortie du sandbox d'Amazon SES). Assurez-vous que l'adresse que vous saisissez est exactement la même que celle que vous avez vérifiée.
- (Facultatif) **`us-west-2`** — Si vous souhaitez utiliser Amazon SES dans une région autre que USA Ouest (Oregon), remplacez ceci par la région que vous souhaitez utiliser. Pour connaître la liste des régions dans lesquelles Amazon SES est disponible, consultez Amazon Simple Email Service (Amazon SES) dans le document Références générales AWS.

3. Enregistrez `amazon-ses-sample.py`.
4. Pour exécuter le programme, ouvrez une invite de commande dans le même répertoire que `amazon-ses-sample.py`, puis entrez python amazon-ses-sample.py.
5. Vérifiez la sortie. Si l'envoi de l'e-mail aboutit, la console affiche «`Email sent!`». Dans le cas contraire, elle affiche un message d'erreur.
6. Connectez-vous au client de messagerie de l'adresse du destinataire. Vous verrez le message que vous avez envoyé.

Création d'un fichier d'informations d'identification partagé à utiliser lors de l'envoi d'e-mails via Amazon SES à l'aide d'un AWS SDK

La procédure suivante montre comment créer un fichier d'informations d'identification partagées dans votre répertoire. Pour que l'exemple de code du kit de développement logiciel (SDK) fonctionne correctement, vous devez créer ce fichier.

1. Dans un éditeur de texte, créez un fichier. Dans le fichier, collez le code suivant :

```
[default]
aws_access_key_id = YOUR_AWS_ACCESS_KEY_ID
aws_secret_access_key = YOUR_AWS_SECRET_ACCESS_KEY
```

2. Dans le fichier texte que vous venez de créer, remplacez-le `YOUR_AWS_ACCESS_KEY` par votre identifiant de clé d' AWS accès unique et remplacez-le `YOUR_AWS_SECRET_ACCESS_KEY` par votre clé d'accès AWS secrète unique.

3. Enregistrez le fichier. Le tableau suivant indique l'emplacement et le nom de fichier corrects pour votre système d'exploitation.

Si vous utilisez…	Enregistrez le fichier sous le nom...
Windows	`C:\Users\<yourUserName>\.aws\credentials`
Linux, macOS ou Unix	`~/.aws/credentials`

> **Important**
>
> N'ajoutez pas d'extension de fichier lors de le registre du fichier des informations d'identification.

Encodages de contenu pris en charge par Amazon SES

Les éléments suivants sont fournis à titre de référence.

Amazon SES prend en charge les codages de contenu suivants :

- `deflate`
- `gzip`
- `identity`

Amazon SES prend également en charge le format d'en-tête Accept-Encoding suivant, conformément à la spécification RFC 7231 :

- `Accept-Encoding:deflate,gzip`
- `Accept-Encoding:`
- `Accept-Encoding:*`
- `Accept-Encoding:deflate;q=0.5,gzip;q=1.0`
- `Accept-Encoding:gzip;q=1.0,identity;q=0.5,*;q=0`

Amazon SES et protocoles de sécurité

Cette rubrique décrit les protocoles de sécurité que vous pouvez utiliser lorsque vous vous connectez à Amazon SES, mais aussi lorsqu'Amazon SES remet un e-mail à un récepteur.

Expéditeur d'e-mails à destination d'Amazon SES

Le protocole de sécurité que vous utilisez pour vous connecter à Amazon SES varie selon que vous utilisez l'API Amazon SES ou l'interface SMTP Amazon SES, comme décrit ensuite.

HTTPS

Si vous utilisez l'API Amazon SES (directement ou via un AWS SDK), toutes les communications sont cryptées par TLS via le point de terminaison HTTPS Amazon SES. Le point de terminaison HTTPS Amazon SES prend en charge TLS 1.2 et TLS 1.3.

Interface SMTP

Si vous accédez à Amazon SES via l'interface SMTP, vous devez chiffrer votre connexion à l'aide du protocole TLS (Transport Layer Security). Notez que TLS est souvent désigné sous le nom de son prédécesseur, le protocole SSL (Secure Sockets Layer).

Amazon SES prend en charge deux mécanismes d'établissement d'une connexion à chiffrement TLS : STARTTLS et TLS Wrapper.

- STARTTLS – STARTTLS permet de mettre à niveau une connexion non chiffrée en connexion chiffrée. Il existe différentes versions de STARTTLS selon les protocoles. La version SMTP est définie dans RFC 3207. Pour les connexions STARTTLS, Amazon SES prend en charge les protocoles TLS 1.2 et TLS 1.3.
- TLS Wrapper – TLS Wrapper (également connu sous le nom de SMTPS ou de protocole de négociation) permet d'initier une connexion chiffrée sans établir en premier lieu une connexion non chiffrée. Avec TLS Wrapper, le point de terminaison SMTP Amazon SES n'effectue pas de négociation TLS : c'est la responsabilité du client de se connecter au point de terminaison à l'aide de TLS et de continuer à utiliser TLS pour la totalité de la conversation. TLS Wrapper est un protocole plus ancien, mais de nombreux clients continuent de le prendre en charge. Pour les connexions TLS Wrapper, Amazon SES prend en charge TLS 1.2 et TLS 1.3.

Pour obtenir des informations sur la connexion à l'interface SMTP Amazon SES à l'aide de ces méthodes, consultez Connexion à un point de terminaison SMTP Amazon SES.

Amazon SES à destination d'un récepteur

SES prend en charge TLS 1.2 pour les connexions TLS. Pour en savoir plus, veuillez consulter la section Sécurité de l'infrastructure dans SES.

Par défaut, Amazon SES utilise la méthode TLS opportuniste. Cela signifie qu'Amazon SES tente toujours de créer une connexion sécurisée au serveur de messagerie de réception. Si Amazon SES ne peut pas établir une connexion sécurisée, il envoie le message non chiffré.

Vous pouvez modifier ce comportement en utilisant des jeux de configurations. Utilisez l'opération PutConfigurationSetDeliveryd'API Options pour définir la `TlsPolicy` propriété d'une configuration définie sur`Require`. Vous pouvez utiliser l'AWS CLI pour effectuer cette modification.

Pour configurer Amazon SES afin d'exiger des connexions TLS pour un jeu de configurations

- Sur la ligne de commande, entrez la commande suivante :

  ```
  aws sesv2 put-configuration-set-delivery-options --configuration-set-
  name MyConfigurationSet --tls-policy REQUIRE
  ```

  Dans l'exemple précédent, remplacez *MyConfigurationSet* par le nom de votre ensemble de configuration.

  Lorsque vous envoyez un e-mail à l'aide de ce jeu de configurations, Amazon SES envoie uniquement le message au serveur de messagerie de réception s'il peut établir une connexion sécurisée. Si Amazon SES ne peut pas créer une connexion sécurisée au serveur de messagerie de réception, il supprime le message.

nd-to-end Chiffrement électronique

Vous pouvez utiliser Amazon SES pour envoyer des messages chiffrés à l'aide de S/MIME ou PGP. Les messages qui utilisent ces protocoles sont chiffrés par l'expéditeur. Leur contenu ne peut être consulté que par les destinataires qui possèdent les clés privées requises pour déchiffrer les messages.

Amazon SES prend en charge les types MIME suivants, que vous pouvez utiliser pour envoyer des e-mails chiffrés à l'aide de S/MIME :

- `application/pkcs7-mime`

- `application/pkcs7-signature`
- `application/x-pkcs7-mime`
- `application/x-pkcs7-signature`

Amazon SES prend également en charge les types MIME suivants, que vous pouvez utiliser pour envoyer des e-mails chiffrés à l'aide de PGP :

- `application/pgp-encrypted`
- `application/pgp-keys`
- `application/pgp-signature`

Champs d'en-tête Amazon SES

Amazon SES accepte tous les champs d'en-tête de-mail qui respectent le format décrit dans RFC 822.

Les champs suivants ne peuvent pas apparaître plusieurs fois dans la section d'en-tête d'un message :

- `Accept-Language`
- `acceptLanguage`
- `Archived-At`
- `Auto-Submitted`
- `Bounces-to`
- `Comments`
- `Content-Alternative`
- `Content-Base`
- `Content-Class`
- `Content-Description`
- `Content-Disposition`
- `Content-Duration`
- `Content-ID`

- Content-Language
- Content-Length
- Content-Location
- Content-MD5
- Content-Transfer-Encoding
- Content-Type
- Date
- Delivered-To
- Disposition-Notification-Options
- Disposition-Notification-To
- DKIM-Signature
- DomainKey-Signature
- Errors-To
- From
- Importance
- In-Reply-To
- Keywords
- List-Archive
- List-Help
- List-Id
- List-Owner
- List-Post
- List-Subscribe
- List-Unsubscribe
- List-Unsubscribe-Post
- Message-Context
- Message-ID
- MIME-Version

- `Organization`
- `Original-From`
- `Original-Message-ID`
- `Original-Recipient`
- `Original-Subject`
- `Precedence`
- `Priority`
- `References`
- `Reply-To`
- `Return-Path`
- `Return-Receipt-To`
- `Sender`
- `Solicitation`
- `Sensitivity`
- `Subject`
- `Thread-Index`
- `Thread-Topic`
- `User-Agent`
- `VBR-Info`

Considérations

- Le champ `acceptLanguage` n'est pas standard. Si possible, utilisez plutôt l'en-tête `Accept-Language`.
- Si vous spécifiez un en-tête `Date`, Amazon SES le remplace par un horodatage correspondant à la date et à l'heure du fuseau horaire UTC auxquelles Amazon SES a accepté le message.
- Si vous fournissez un en-tête `Message-ID`, Amazon SES remplace cet en-tête par sa propre valeur.
- Si vous spécifiez un en-tête `Return-Path`, Amazon SES envoie les notifications de retour à l'expéditeur et de réclamation à l'adresse que vous avez spécifiée. Toutefois, le message que vos destinataires reçoivent contient une valeur différente pour l'en-tête `Return-Path`.

- Si vous utilisez l'`SendEmail`opération Amazon SES API v2 avec du contenu simple ou modélisé, ou si vous utilisez l'`SendBulkEmail`opération, vous ne pouvez pas définir de contenu d'en-tête personnalisé pour les en-têtes définis par SES ; par conséquent, les en-têtes suivants ne sont pas autorisés en tant qu'en-têtes personnalisés :
  - `BCC`, `CC`, `Content-Disposition`, `Content-Type`, `Date`, `From`, `Message-ID`, `MIME-Version`, `Reply-To`, `Return-Path`, `Subject`, `To`

Types de pièces jointes non pris en charge par Amazon SES

Vous pouvez envoyer des messages avec des pièces jointes via Amazon SES en utilisant le standard Multipurpose Internet Mail Extensions (MIME). Amazon SES accepte tous les types de pièces jointes à l'exception des pièces jointes dont l'extension de fichier figure dans la liste qui suit.

.ade	.hta	.mau	.mst	.psc1
.adp	.inf	.mav	.ops	.psc2
.app	.ins	.maw	.pcd	.tmp
.asp	.isp	.mda	.pif	.url
.bas	.its	.mdb	.plg	.vb
.bat	.js	.mde	.prf	.vbe
.cer	.jse	.mdt	.prg	.vbs
.chm	.ksh	.mdw	.reg	.vps
.cmd	.lib	.mdz	.scf	.vsmacros
.com	.lnk	.msc	.scr	.vss
.cpl	.mad	.msh	.sct	.vst
.crt	.maf	.msh1	.shb	.vsw
.csh	.mag	.msh2	.shs	.vxd
.der	.mam	.mshxml	.sys	.ws

.exe	.maq	.msh1xml	.ps1	.wsc
.fxp	.mar	.msh2xml	.ps1xml	.wsf
.gadget	.mas	.msi	.ps2	.wsh
.hlp	.mat	.msp	.ps2xml	.xnk

Certains fournisseurs de services Internet (ISP) ayant d'autres restrictions (par exemple, en matière de pièces jointes archivées), nous vous recommandons de tester votre envoi d'e-mails via les principaux ISP avant d'envoyer votre e-mail de production.

Réception d'e-mails avec Amazon SES

En plus d'Amazon SES pour gérer votre envoi d'e-mails, vous pouvez également configurer SES pour recevoir des e-mails au nom d'un ou de plusieurs de vos domaines. En tant que récepteur d'e-mails, SES gère les opérations de réception d'e-mails de base, telles que la communication avec d'autres serveurs de messagerie, l'analyse des spams et des virus, le blocage des e-mails provenant de sources non fiables (adresses des listes de blocage Spamhaus ou SES) et l'acceptation des e-mails pour les destinataires de votre domaine.

Le traitement de votre e-mail reçu est déterminée par les instructions personnalisées que vous spécifiez. Ces instructions se présentent sous deux formes :

- Règles de réception (contrôle fondé sur le bénéficiaire) fournissent les meilleurs détails de contrôle sur les e-mails entrants. Les règles de réception peuvent effectuer un traitement avancé, comme envoyer le courrier entrant à un compartiment Amazon S3, le publier dans une rubrique Amazon SNS, l'envoyer à Amazon WorkMail ou envoyer automatiquement des messages de retour à l'expéditeur lorsque les messages sont envoyés à des adresses e-mail spécifiques, etc.
- Filtres d'adresse IP d' (Contrôle basé sur l'IP) offrent un large niveau de contrôle et sont simples à configurer. Ces filtres vous permettent de bloquer ou d'autoriser explicitement tous les messages provenant d'adresses IP ou de plages d'adresses IP spécifiques.

Pour commencer à recevoir des e-mails, à les configurer et à les implémenter à l'aide de Règles de réception ou Filtres d'adresse IP, d'abord lu via Concepts de réception d'e-mails et cas d'utilisation pour obtenir un aperçu de son fonctionnement et des différentes façons de l'utiliser. Ensuite, Configuration de la réception d'e-mails vous guidera à travers les conditions préalables de la réception des e-mails. Ensuite, Instructions pour la console de réception d'e-mails vous guidera tout au long des assistants utilisés pour la configuration Règles de réception et Filtres d'adresse IP.

> **Note**
>
> La réception d'e-mails ne peut être utilisée que si votre compte se trouve dans une Région AWS dans laquelle SES prend en charge la réception d'e-mails. Consultez Régions de réception d'e-mails prises en charge par SES.

Rubriques de cette section :

Concepts de réception d'e-mails et cas d'utilisation Amazon SES

Lorsque vous utilisez Amazon SES comme serveur de messagerie, vous indiquez au service ce qu'il doit faire avec vos messages. La première méthode, les règles de réception, vous permet de contrôler avec précision la réception de vos e-mails en utilisant le contrôle basé sur le destinataire pour spécifier un ensemble d'actions à entreprendre en fonction du destinataire. L'autre méthode, les filtres d'adresses IP, fournit un large niveau decontrôle basé sur l'IP pour bloquer ou autoriser les messages en fonction de l'adresse IP d'origine ou de la plage d'adresses.

Ces deux méthodes sont décrites dans cette section, avec un aperçu de la façon dont Amazon SES traite le message reçu, et des cas d'utilisation pour vous aider à déterminer comment vous souhaitez recevoir, filtrer et traiter votre message lors de la configuration des règles et des filtres.

Rubriques de cette section :

Contrôle basé sur le destinataire à l'aide de règles de réception

Le principal moyen de contrôler votre message entrant est de spécifier la façon dont il est traité grâce à une liste détaillée d'actions pour toutes vos identités vérifiées, à savoir vos domaines, sous-domaines ou adresses e-mail. Notez que les adresses e-mail doivent appartenir à l'une de vos identités de domaine vérifiées. Ces actions sont définies et ordonnées dans les règles de réception que vous créez dans un ensemble de règles.

En option, vous pouvez également ajouter des conditions au destinataire pour spécifier que les actions ne doivent être exécutées que si le destinataire du message entrant correspond à une identité

de destinataire indiquée dans la condition. Par exemple, si vous possédez exemple.com, vous pouvez spécifier que les messages destinés à utilisateur@exemple.com doivent être renvoyés à l'expéditeur et que tous les autres messages pour exemple.com et ses sous-domaines doivent être livrés.

Si vous n'ajoutez aucune condition de destinataire, les actions seront appliquées à toutes les adresses e-mail, domaines et sous-domaines qui appartiennent à vos domaines vérifiés. Les actions suivantes peuvent être appliquées à vos règles de réception :

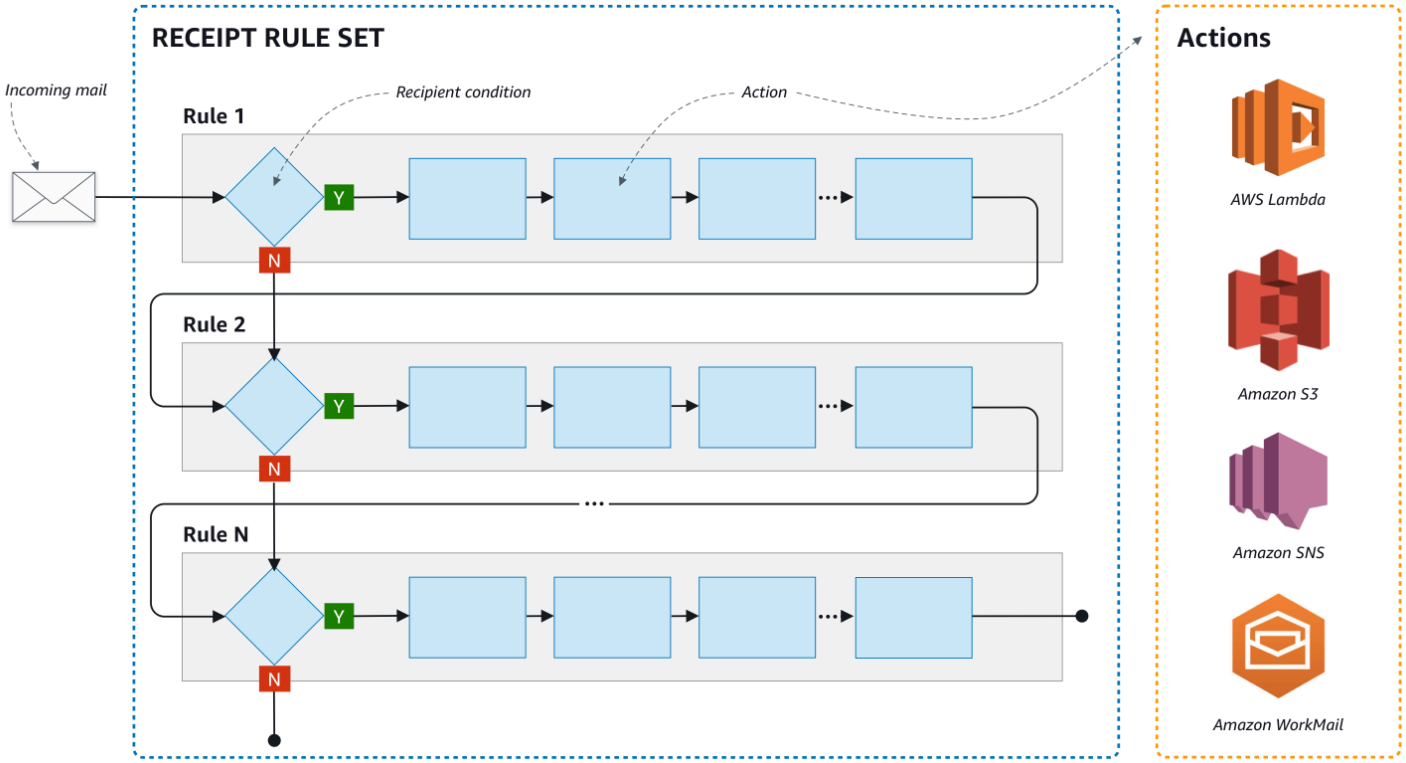
- Action Add header (Ajout d'en-tête) – Ajoute un en-tête à l'e-mail reçu. Vous utilisez généralement cette action uniquement en combinaison avec d'autres actions.
- Return bounce response action (Action de réponse de retour à l'expéditeur) : bloque l'e-mail en renvoyant une réponse de retour à l'expéditeur et vous avertit éventuellement via Amazon SNS.
- Invoquer l'action de fonction Lambda (Invoke AWS Lambda function action) – Appelle votre code via une fonction Lambda et vous avertit éventuellement via Amazon SNS.
- Deliver to S3 bucket action (Livrer à l'action du compartiment S3) – Place les messages dans un compartiment Amazon S3 et vous avertit éventuellement via Amazon SNS.
- Publish to Amazon SNS topic action (Publier sur une action de rubrique Amazon SNS) — Publie l'e-mail complet dans une rubrique Amazon SNS.

> **Note**
>
> L'action SNS comprend une copie complète du contenu des e-mails dans les notifications Amazon SNS. Les autres options de notifications Amazon SNS mentionnées ici vous informent simplement de la remise d'un e-mail ; elles contiennent des informations sur l'e-mail, et non le contenu de l'e-mail proprement dit.

- Stop rule set action Action Stop (Arrêter l'action du jeu de règles) – Met fin à l'évaluation de l'ensemble de règles de réception et vous avertit éventuellement via Amazon SNS.
- Integrate with Amazon WorkMail action (Intégrer l'action Amazon WorkMail) – Traite les messages avec Amazon WorkMail. Vous n'utilisez généralement pas cette action directement, car Amazon WorkMail se charge de la configuration.

Les règles de réception sont regroupées en jeux de règles. Si vous n'avez pas de jeu de règles existant, vous devez d'abord créer un jeu de règles avant de commencer à créer des règles de réception. Vous pouvez définir plusieurs ensembles de règles pour votre compte AWS, mais un seul

ensemble est actif à un moment donné. La figure suivante illustre les relations entre les règles, les ensembles de règles de réception et les actions.



Contrôle basé sur IP à l'aide de filtres d'adresses IP

Vous pouvez contrôler votre flux de messagerie en configurant des filtres d'adresses IP. Les filtres d'adresses IP sont facultatifs et vous permettent de choisir d'accepter ou de bloquer les messages provenant d'une adresse IP ou d'une plage d'adresses IP. Vos filtres d'adresses IP peuvent inclure des listes rouges (adresses IP dont vous souhaitez bloquer les messages entrants) et des listes vertes (adresses IP dont vous souhaitez toujours accepter les messages).

Les filtres d'adresses IP sont utiles pour bloquer le courrier indésirable. Amazon SES gère sa propre liste de blocage d'adresses IP connues pour envoyer du courrier indésirable, notamment elles répertoriées dans Spamhaus. Toutefois, vous pouvez choisir de recevoir les messages provenant de ces adresses IP en ajoutant celles-ci à votre liste d'autorisations. Étant donné qu'aucun journal n'indique les adresses IP qui sont bloquées, l'expéditeur bloqué devra vous en informer. Il s'agit également d'une bonne occasion d'aider l'expéditeur à déterminer si son adresse IP figure sur une liste de blocage, par exemple Spamhaus, et de lui recommander de demander à être supprimé de la liste. Cela sera bénéfique pour vous et pour l'expéditeur, car vous n'aurez pas à gérer un filtre d'adresse IP pour lui et cela améliorera la délivrabilité de ses e-mails.

> **Note**
>
> - Indépendamment de votre configuration de filtres d'adresses IP, Amazon EC2 bloque le trafic sortant sur le port 25 (envoi de courrier) sauf s'il figure dans la liste d'autorisation. Consultez cet article AWS re:Post pour en savoir plus.
> - Si vous souhaitez uniquement recevoir des messages à partir d'une liste finie d'adresses IP connues, configurez une liste rouge qui contient `0.0.0.0/0` et une liste verte qui contient les adresses IP que vous approuvez. Cette configuration bloque toutes les adresses IP par défaut, et autorise uniquement les messages provenant des adresses IP que vous spécifiez explicitement.

Processus de réception des messages

Lorsqu'Amazon SES reçoit un e-mail pour votre domaine, les événements suivants ont lieu :

1. Amazon SES examine d'abord l'adresse IP de l'expéditeur. Amazon SES autorise l'e-mail à réussir cette étape sauf dans les cas suivants :
   - L'adresse IP figure dans votre liste rouge.
   - L'adresse IP figure dans la liste rouge d'Amazon SES mais n'est pas dans votre liste verte.
2. Amazon SES examine votre jeu de règles actif pour déterminer si l'une de vos règles de réception contient une condition de destinataire :
   - S'il existe une condition de destinataire et qu'elle correspond à l'un des destinataires de l'e-mail entrant, Amazon SES accepte l'e-mail. S'il n'y a pas de correspondance, Amazon SES bloque l'e-mail.
   - Si la règle de réception ne contient pas de condition de destinataire, Amazon SES accepte le message et toutes les actions de la règle s'appliqueront à toutes les identités vérifiées que vous possédez.
3. Amazon SES authentifie l'e-mail et vérifie s'il s'agit d'un courrier indésirable et recherche des logiciels malveillants :
   - L'adresse IP de l'hôte distant qui a livré l'e-mail à Amazon SES est vérifiée par rapport à la stratégie SPF spécifiée sous le domaine MAIL FROM utilisé lors de la transaction SMTP.
   - Les signatures DKIM présentes dans la section d'en-tête de l'e-mail sont vérifiées.
   - Si l'analyse du contenu est activée, le contenu de l'e-mail est analysé pour y vérifier s'il s'agit d'un courrier indésirable et détecter des logiciels malveillants.

- Les résultats de l'authentification d'e-mail et de l'analyse de contenu sont mis à votre disposition lors de l'évaluation des règles de réception.

Pour plus d'informations, consultez Authentification d'e-mails et détection de logiciels malveillants.

4. Pour l'e-mail qu'Amazon SES accepte, toutes les règles de réception de votre jeu de règles actif sont appliquées dans l'ordre que vous avez défini et, dans chaque règle de réception, les actions sont exécutées dans l'ordre que vous avez défini.

Cas d'utilisation et restrictions pour la réception d'e-mails Amazon SES

Cette section passe en revue quelques considérations générales et cas d'utilisation pour la réception d'emails Amazon SES. Sous forme de questions et réponses, vous trouverez des questions fréquemment posées et des informations qui vous aideront à déterminer s'il est avantageux d'utiliser Amazon SES pour recevoir et gérer les e-mails au nom d'un ou de plusieurs domaines vérifiés que vous possédez.

Disponibilité par région

La réception des e-mails dans votre région est-elle prise en charge par Amazon SES ?

Amazon SES ne prend en charge la réception d'e-mails que dans certaines régions AWS. Pour obtenir la liste complète des régions prenant en charge la réception d'e-mails, veuillez consulter Points de terminaison et quotas Amazon Simple Email Service dans le document Références générales AWS.

Clients de messagerie POP ou IMAP

Microsoft Outlook peut-il être utilisé pour recevoir des e-mails entrants ?

Amazon SES n'inclut pas les serveurs POP ou IMAP pour recevoir les e-mails entrants. Ceci signifie que vous ne pouvez pas utiliser un client de messagerie tel que Microsoft Outlook pour recevoir des e-mails entrants. Si vous souhaitez une solution qui peut envoyer et recevoir des e-mails à l'aide d'un client de messagerie, pensez à utiliser Amazon WorkMail.

Utilisation d'autres services AWS

Avez-vous configuré les autorisations appropriées ?

Si vous voulez que vos messages soient remis à un compartiment S3, qu'ils soient publiés dans une rubrique Amazon SNS que vous ne possédez pas, qu'ils déclenchent une fonction Lambda ou qu'ils

utilisent une clé gérée personnalisée, vous devez autoriser Amazon SES à accéder à ces ressources. Pour accorder ces accès à Amazon SES, vous créez des stratégies sur des ressources à partir des consoles ou des API pour ces services AWS. Pour en savoir plus Attribution d'autorisations.

Contenu des e-mails

Comment souhaitez-vous qu'Amazon SES vous transmette le contenu des e-mails?

Amazon SES peut vous fournir le contenu des e-mails de deux manières : le service peut stocker les e-mails dans un compartiment S3 que vous spécifiez, ou il peut vous envoyer une notification Amazon SNS qui contient une copie de l'e-mail. Amazon SES vous remet l'e-mail brut non modifié au format Multipurpose Internet Mail Extensions (MIME). Pour plus de détails sur le format MIME, consultez la spécification RFC 2045.

Quelle est la taille des e-mails que vous recevrez ?

Si vous stockez des e-mails dans un compartiment S3, la taille maximale des e-mails (en-têtes compris) est de 40 Mo. Si vous décidez de recevoir vos e-mails via des notifications Amazon SNS, la taille maximale des e-mails (en-têtes compris) est de 150 Ko.

Comment voulez-vous déclencher le traitement de vos e-mails ?

Une fois que votre e-mail est remis, vous souhaiterez le traiter avec votre propre code. Par exemple, votre application peut convertir les e-mails encodés en base 64 dans un format affichable, puis les mettre à disposition d'un utilisateur final via un client de messagerie. Vous pouvez démarrer le processus de deux façons :

- Si vos e-mails sont remis à Amazon S3, votre application peut écouter les notifications Amazon SNS générées par les actions S3, extraire l'ID de message de l'e-mail à partir des notifications, puis utiliser cet ID pour récupérer l'e-mail depuis Amazon S3.

  Sinon, vous pouvez intégrer le traitement des e-mails dans vos règles de réception en écrivant une fonction Lambda. Dans ce cas, votre règle de réception doit d'abord écrire l'e-mail dans Amazon S3, puis déclencher la fonction Lambda. Des actions Lambda peuvent être exécutées de manière synchrone ou asynchrone depuis vos règles de réception, selon que la fonction Lambda doit renvoyer un résultat qui détermine comment d'autres actions sont effectuées. Nous vous conseillons d'utiliser l'exécution asynchrone, sauf si une exécution synchrone est absolument nécessaire à votre cas d'utilisation. Pour en savoir plus sur AWS Lambda, consultez le Guide du développeur AWS Lambda.

- Si vos e-mails sont remis via une notification Amazon SNS à l'aide de l'action SNS, votre application peut écouter les notifications Amazon SNS, puis extraire les e-mails des notifications.

Souhaitez-vous que les e-mails soient chiffrés ?

Amazon SES s'intègre à AWS Key Management Service (AWS KMS) afin de chiffrer éventuellement les messages qu'il écrit dans votre compartiment S3. Amazon SES utilise le chiffrement côté client pour chiffrer vos messages avant de les écrire dans Amazon S3. Cela signifie que vous devez déchiffrer le contenu de votre côté après avoir récupéré les messages depuis Amazon S3. Le kit AWS SDK for Java et le kit AWS SDK for Ruby fournissent un client qui peut traiter le déchiffrement pour vous. Amazon SES peut chiffrer les e-mails pour vous uniquement si vous choisissez que vos e-mails soient remis dans un compartiment S3.

Courrier indésirable

À quel stade du processus de réception d'e-mails souhaitez bloquer le courrier indésirable ?

Lorsque l'expéditeur tente d'envoyer un e-mail à un destinataire, le serveur de messagerie de l'expéditeur échange une séquence de commandes avec le serveur du destinataire. Cette séquence est appelée conversation SMTP.

Vous pouvez bloquer un e-mail entrant à deux moments au cours du processus de réception des e-mails : au cours de la conversation SMTP et après la conversation SMTP. Vous utilisez les filtres d'adresses IP pour bloquer les messages au cours de la conversation SMTP et les règles de réception pour bloquer les e-mails après la conversation SMTP.

Vous pouvez utiliser les filtres d'adresses IP pour bloquer les e-mails provenant d'adresses IP spécifiques. L'avantage de l'utilisation des filtres d'adresses IP pour bloquer le courrier indésirable est que nous ne vous facturerons pas les messages bloqués au cours de la conversation SMTP. L'inconvénient de l'utilisation des filtres d'adresses IP est qu'ils bloquent les e-mails provenant des adresses IP que vous spécifiez sans exécuter la moindre analyse sur le contenu des messages. Pour en savoir plus sur les filtres des adresses IP, consultez Création de filtres d'adresses IP - Démonstration de la console.

Vous pouvez utiliser les règles de réception pour envoyer une notification de retour à l'expéditeur d'un e-mail en fonction de l'adresse (ou du domaine ou sous-domaine) à laquelle le message a été envoyé. L'avantage de l'utilisation des règles de réception est que vous pouvez effectuer une analyse supplémentaire des messages entrants avant d'envoyer une notification de retour à l'expéditeur. Par exemple, vous pouvez utiliser AWS Lambda pour envoyer des notifications de retour

à l'expéditeur uniquement lorsque les messages échouent à l'authentification DKIM ou sont identifiés comme courrier indésirable. L'inconvénient de l'utilisation de règles de réception est que, dans la mesure où les règles de réception sont traitées après la conversation SMTP, nous vous facturons chaque message que vous recevez. Vous pouvez également être facturé si vous utilisez Lambda pour analyser le contenu des messages entrants. Pour en savoir plus sur les règles de réception, consultez Création de règles de réception - Démonstration de la console. Pour en savoir plus sur l'utilisation de Lambda pour analyser les e-mails entrants, consultez Exemples de fonctions Lambda.

Flux de messagerie

Comment voulez-vous répartir vos flux de messagerie ?

Votre domaine reçoit très probablement différentes classes de messages. Par exemple, une partie des messages de votre domaine, comme un e-mail envoyé à utilisateur@exemple.com, peut être destinée à une boîte de réception personnelle. Il serait préférable pour d'autres messages, comme un e-mail envoyé à unsubscribe@exemple.com, d'être plutôt dirigés vers des systèmes automatisés. Vous pouvez utiliser des règles de réception pour répartir vos messages entrants de façon à ce qu'ils puissent être traités différemment. Pour en savoir plus sur la configuration de règles de réception, consultez Création de règles de réception.

Authentification de la réception d'e-mails et recherche de logiciels malveillants

Amazon SES authentifie chaque e-mail reçu et y vérifie éventuellement s'il s'agit d'un courrier indésirable et s'il contient des logiciels malveillants : SES n'effectue aucune action sur les e-mails reçus en fonction des résultats de l'authentification d'e-mail ou de l'analyse de contenu. En revanche, les résultats de ces opérations vous sont fournis sous la forme d'attributs que vous pouvez utiliser dans les actions de règles de réception SES, telles que les Amazon SNS notifications (Notifications Amazon SNS) ou comme en-têtes dans un message remis dans Amazon S3.

Authentification d'e-mail

Amazon SES authentifie chaque e-mail reçu à l'aide de SPF, DKIM et DMARC. Les résultats de chaque mécanisme d'authentification sont fournis dans les notifications Amazon SNS envoyées par SES dans le cadre de l'évaluation des règles dans l'ensemble de règles de réception actif. Par ailleurs, si vous avez choisi de recevoir une copie de l'e-mail dans Amazon S3, le résultat de l'authentification d'e-mail est capturé dans l'en-tête `Authentication-Results` que SES ajoute à la section d'en-tête de l'e-mail :

```
Authentication-Results: example.com;
spf=pass (spfCheck: 10.0.0.1 is permitted by domain of example.com) client-ip=10.0.0.1;
 envelope-from=example@example.com; helo=10.0.0.1;
dkim=pass header.i=example.com;
dkim=permerror header.i=some-example.com;
dmarc=pass header.from=example@example.com;
```

L'en-tête `Authentication-Results` est décrit dans RFC 8601

Analyse du contenu d'e-mail pour détecter le courrier indésirable et les logiciels malveillants

Amazon SES analyse le contenu des e-mails reçus à la recherche de logiciels malveillants en fonction de la valeur de l'attribut ScanEnabled (API) ou Spam and virus scanning (Analyse anti-spam et virus) (console) de la règle de réception associée à l'e-mail. Par défaut, SES recherche les logiciels malveillants dans le contenu des e-mails. Pour désactiver l'analyse de contenu des e-mails reçus qui correspondent à une règle de réception spécifique, vous devez définir l'indicateur ScanEnabled de la règle de réception sur false si vous utilisez l'API ou désactiver la case Spam and virus scanning (Analyse anti-spam et virus) si vous utilisez la console. Si la règle de réception correspondant à un e-mail est activée, le résultat de l'analyse du contenu est fourni dans les notifications Amazon SNS envoyées par SES dans le cadre de l'évaluation des règles de l'ensemble de règles de réception actif. Par ailleurs, si vous avez choisi de recevoir une copie de l'e-mail dans Amazon S3, le résultat de l'analyse du contenu est capturé dans les en-têtes `X-SES-Spam-Verdict` et `X-SES-Virus-Verdict` que SES ajoute à la section d'en-tête de l'e-mail

```
X-SES-Spam-Verdict: PASS
X-SES-Virus-Verdict: FAIL
```

Les valeurs possibles pour les en-têtes ci-dessus sont répertoriées dans :

- spam
- virus

Maintenant que vous avez compris les concepts de la réception d'e-mails, son fonctionnement et ses cas d'utilisation, vous pouvez commencer en allant sur Configuration de la réception d'e-mails.

Configuration de la réception d'e-mails via Amazon SES

Cette section décrit les conditions préalables requises avant de pouvoir commencer à configurer Amazon SES pour recevoir votre e-mail. Il est important de lire Concepts de réception d'e-mails et cas d'utilisation pour comprendre les concepts du fonctionnement d'Amazon SES et pour réfléchir à la manière dont vous souhaitez recevoir, filtrer et traiter votre e-mail.

Avant de pouvoir configurer la réception des e-mails en créant un jeu de règles, des règles de réception et des filtres d'adresse IP, vous devez d'abord remplir les conditions préalables suivantes :

- Vérifiez votre domaine avec Amazon SES en publiant des registres DNS pour prouver que vous en êtes le propriétaire.
- Autorisez Amazon SES à recevoir des e-mails pour votre domaine en publiant un registre MX.
- Autoriser Amazon SES à accéder à d'autres ressources AWS afin d'exécuter des actions de règle de réception.

Lorsque vous créez et vérifiez l'identité d'un domaine, vous publiez des registres dans vos paramètres DNS pour achever le processus de vérification, mais cela ne suffit pas pour utiliser la réception d'e-mails. En ce qui concerne la réception d'e-mails, il est également nécessaire de publier un registre MX pour spécifier un domaine personnalisé de réception d'e-mails. Cet registre est utilisé dans les paramètres DNS de votre domaine pour permettre à SES de recevoir des e-mails pour votre domaine. Les autorisations sont nécessaires car les actions que vous choisissez dans vos règles de réception ne fonctionneront pas si Amazon SES n'a pas l'autorisation d'utiliser le service AWS requis pour ces actions.

Ces trois conditions préalables nécessaires à l'utilisation de la réception d'e-mails sont expliquées dans les rubriques suivantes :

- Vérification de votre domaine pour la réception d'e-mails via Amazon SES
- Publication d'un registre MX pour la réception d'e-mails via Amazon SES
- Attribution d'autorisations à Amazon SES pour la réception d'e-mails

Vérification de votre domaine pour la réception d'e-mails via Amazon SES

Comme avec tout domaine que vous voulez utiliser pour envoyer ou recevoir des e-mails avec Amazon SES, vous devez d'abord prouver que vous possédez ce domaine. La procédure de vérification comprend le lancement de la vérification de domaine avec SES, puis la publication de

registres DNS (CNAME ou TXT) sur votre fournisseur DNS, en fonction de la méthode de vérification utilisée.

Grâce à la console, vous pouvez vérifier vos domaines à l'aide de Easy DKIM ou Bring Your Own DKIM (BYODKIM) et copier facilement leurs registres DNS pour les publier sur votre fournisseur DNS. La procédure à suivre est décrite dans Création d'une identité de domaine. Vous pouvez également utiliser les API SES `VerifyDomainDkim` ou `VerifyDomainIdentity`.

Vous pouvez facilement confirmer que votre adresse e-mail ou votre domaine est bien vérifié en examinant son statut dans le tableau Verified identities (Identités vérifiées) de la console SES ou à l'aide des API SES `GetIdentityVerificationAttributes` ou `GetEmailIdentity`.

Publication d'un registre MX pour la réception d'e-mails via Amazon SES

Un registre d'échangeur de messagerie (MX) est une configuration qui spécifie les serveurs de messagerie pouvant accepter les e-mails envoyés à votre domaine.

Pour qu'Amazon SES gère vos e-mails entrants, ajoutez un registre MX à la configuration DNS de votre domaine. Le registre MX que vous créez fait référence au point de terminaison de réception d'e-mails pour la région AWS dans laquelle vous utilisez Amazon SES. Par exemple, le point de terminaison de la région USA Ouest (Oregon) est inbound-smtp.us-west-2.amazonaws.com. Pour obtenir la liste complète des points de terminaison, consultez Régions et points de terminaison Amazon SES.

> **Note**
>
> Les points de terminaison recevant les e-mails dans Amazon SES ne sont pas des serveurs de messagerie POP3 ou IMAP. Vous ne pouvez pas utiliser ces URL en tant que serveurs de messagerie entrante dans les clients de messagerie.
> Si vous souhaitez une solution qui peut envoyer et recevoir des e-mails à l'aide d'un client de messagerie, pensez à utiliser Amazon WorkMail.

La procédure suivante inclut les étapes générales de la création d'un registre MX. Les procédures spécifiques de création d'un registre MX dépendent de votre fournisseur DNS ou d'hébergement. Consultez la documentation de votre fournisseur Pour en savoir plus sur l'ajout d'un registre MX à la configuration DNS de votre domaine.

> **Note**
>
> Pour terminer la procédure suivante, vous devez être en mesure de modifier les registres DNS de votre domaine. Si vous ne pouvez pas accéder aux registres DNS de votre domaine, ou que vous n'êtes pas à l'aise pour le faire, contactez votre administrateur système afin d'obtenir de l'aide.

Pour ajouter un registre MX à la configuration DNS de votre domaine

1. Connectez-vous à la console de gestion de votre fournisseur DNS.
2. Créer un registre MX
3. Pour le Name (Nom) de l'enregistrement MX, saisissez votre domaine. Par exemple, si vous souhaitez qu'Amazon SES gère l'e-mail envoyé au domaine example.com, saisissez ce qui suit :

   ```
   example.com
   ```

   > **Note**
   >
   > Certains fournisseurs DNS font référence au champ Name (Nom) en tant que Host (Hôte), Domain (Domaine) ou Mail Domain (Domaine de messagerie).

4. Pour Type, choisissez MX.

   > **Note**
   >
   > Certains fournisseurs DNS font référence au champ Type en tant que Type d' registre ou nom similaire.

5. Dans Value (Valeur), entrez le champ suivant :

   ```
   10 inbound-smtp.region.amazonaws.com
   ```

   Dans l'exemple précédent, remplacez *`region`* par l'adresse du point de terminaison qui reçoit les e-mails de la région AWS que vous utilisez avec Amazon SES. Par exemple, si vous utilisez la région USA Est (Virginie du Nord), remplacez *`region`* par `us-east-1`. Pour obtenir la liste

des points de terminaison de la réception d'e-mails, consultez Régions et points de terminaison Amazon SES.

> **Note**
>
> Les consoles de gestion de certains fournisseurs DNS incluent des champs distincts pour le registre Value (Valeur) et le registre Priority (Priorité). Si tel est le cas de votre fournisseur DNS, saisissez `10` comme valeur pour Priority (Priorité) et entrez l'URL du point de terminaison des messages entrants pour Value (Valeur).

Instructions de création des registres MX pour divers fournisseurs

Les procédures de création d'un registre MX pour votre domaine varient en fonction du fournisseur DNS utilisé. Cette section comprend des liens menant à la documentation proposée par plusieurs fournisseurs DNS courants. Il ne s'agit pas d'une liste exhaustive de fournisseurs. Si votre fournisseur n'est pas répertorié ci-dessous, vous pouvez probablement continuer de l'utiliser avec Amazon SES. L'inclusion dans cette liste ne constitue ni une approbation ni une recommandation vis à vis des produits ou services de l'entreprise.

Nom du fournisseur DNS/d'hébergement	Lien vers la documentation
Amazon Route 53	Création de registres à l'aide de la console Amazon Route 53
GoDaddy	Ajouter un registre MX (lien externe)
DreamHost	Comment puis-je modifier mes registres MX ? (lien externe)
Cloudflare	Configuration des enregistrements d'e-mails (lien externe)
HostGator	Modification des registres MX - Windows (lien externe)

Nom du fournisseur DNS/d'hébergement	Lien vers la documentation
Namecheap	Comment puis-je configurer les registres MX requis pour le service de messagerie ? (lien externe)
Names.co.uk	Modification des paramètres DNS de votre domaine (lien externe)
Wix	Ajout ou mise à jour des registres MX de votre compte Wix (lien externe)

Attribution d'autorisations à Amazon SES pour la réception d'e-mails

Certaines des tâches que vous pouvez effectuer lorsque vous recevez des e-mails dans Amazon SES, telles que l'envoi d'e-mails à un compartiment Amazon Simple Storage Service (Amazon S3) ou l'appel d'une fonction AWS Lambda, nécessitent des autorisations spéciales. Cette section inclut des exemples de stratégies pour plusieurs cas d'utilisation courants.

Rubriques de cette section :

- Attribuer à Amazon SES l'autorisation d'écrire dans un compartiment S3
- Attribuer à Amazon SES l'autorisation d'utiliser votre clé AWS KMS
- Attribuer à Amazon SES l'autorisation d'appeler votre fonction AWS Lambda
- Attribuer à Amazon SES l'autorisation de publier dans une rubrique Amazon SNS qui appartient à un autre compte AWS

Attribuer à Amazon SES l'autorisation d'écrire dans un compartiment S3

Lorsque vous appliquez la stratégie suivante à un compartiment S3, elle autorise Amazon SES à écrire dans ce compartiment. Pour en savoir plus sur la création de règles de réception qui transfèrent les messages entrants vers Amazon S3, consultez Livrer à l'action du compartiment S3.

Pour de plus amples informations sur l'attachement de stratégies de compartiment vers S3, veuillez consulter Stratégies de compartiment et stratégies d'utilisateur dans le Guide de l'utilisateur d'Amazon Simple Storage Service.

```
{
```

```
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AllowSESPuts",
      "Effect":"Allow",
      "Principal":{
        "Service":"ses.amazonaws.com"
      },
      "Action":"s3:PutObject",
      "Resource":"arn:aws:s3:::myBucket/*",
      "Condition":{
        "StringEquals":{
          "AWS:SourceAccount":"111122223333",
          "AWS:SourceArn": "arn:aws:ses:region:111122223333:receipt-rule-
set/rule_set_name:receipt-rule/receipt_rule_name"
        }
      }
    }
  ]
}
```

Dans l'exemple précédent, apportez les modifications suivantes :

- Remplacez *myBucket* par le nom du compartiment S3 dans lequel vous souhaitez écrire.
- Remplacez *region* par la région AWS où vous avez créé la règle de réception.
- Remplacez *111122223333* par votre ID de compte AWS.
- Remplacez *rule_set_name* par le nom du jeu de règles qui contient la règle de réception dans laquelle figure l'action de livraison au compartiment Amazon S3.
- Remplacez *receipt_rule_name* par le nom de la règle de réception contenant l'action de livraison au compartiment Amazon S3.

Attribuer à Amazon SES l'autorisation d'utiliser votre clé AWS KMS

Pour qu'Amazon SES chiffre vos e-mails, le service doit être autorisé à utiliser la clé AWS KMS que vous avez spécifiée lorsque vous avez configuré votre règle de réception. Vous pouvez utiliser la clé KMS par défaut (aws/ses) de votre compte ou une clé gérée par le client que vous créez. Si vous utilisez la clé KMS par défaut, vous n'avez pas besoin d'effectuer des étapes supplémentaires pour autoriser Amazon SES l'utiliser. Si vous utilisez une clé gérée par le client, vous devez attribuer à Amazon SES l'autorisation d'utiliser celle-ci en ajoutant une déclaration dans la stratégie de la clé.

Utilisez la déclaration de stratégie suivante comme stratégie de clé pour autoriser Amazon SES à utiliser votre clé gérée par le client lorsqu'Amazon SES reçoit des e-mails sur votre domaine.

```
{
  "Sid": "AllowSESToEncryptMessagesBelongingToThisAccount",
  "Effect": "Allow",
  "Principal": {
    "Service":"ses.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey*"
  ],
  "Resource": "*",
  "Condition":{
        "StringEquals":{
          "AWS:SourceAccount":"111122223333",
          "AWS:SourceArn": "arn:aws:ses:region:111122223333:receipt-rule-
set/rule_set_name:receipt-rule/receipt_rule_name"
        }
      }
}
```

Dans l'exemple précédent, apportez les modifications suivantes :

- Remplacez *region* par la région AWS où vous avez créé la règle de réception.
- Remplacez *111122223333* par votre ID de compte AWS.
- Remplacez *rule_set_name* par le nom du jeu de règles qui contient la règle de réception que vous avez associée à la réception d'un e-mail.
- Remplacez *receipt_rule_name* par le nom de la règle de réception que vous avez associée à la réception d'e-mails.

Si vous utilisez AWS KMS pour envoyer des messages chiffrés à un compartiment S3 avec le chiffrement côté serveur activé, vous devez ajouter l'action de stratégie, `"kms:Decrypt"`. À l'aide de l'exemple précédent, l'ajout de cette action à votre stratégie s'affiche comme suit :

```
{
  "Sid": "AllowSESToEncryptMessagesBelongingToThisAccount",
  "Effect": "Allow",
  "Principal": {
    "Service":"ses.amazonaws.com"
```

```
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*",
  "Condition":{
        "StringEquals":{
          "AWS:SourceAccount":"111122223333",
          "AWS:SourceArn": "arn:aws:ses:region:111122223333:receipt-rule-
set/rule_set_name:receipt-rule/receipt_rule_name"
        }
      }
}
```

Pour en savoir plus sur l'attachement de stratégies aux clés AWS KMS, consultez Utilisation de stratégies de clé dans AWS KMS dans le Guide du développeur AWS Key Management Service.

Attribuer à Amazon SES l'autorisation d'appeler votre fonction AWS Lambda

Pour permettre à Amazon SES d'appeler une fonction AWS Lambda, vous pouvez choisir la fonction lorsque vous créez une règle de réception dans la console Amazon SES. Lorsque vous le faites, Amazon SES ajoute automatiquement les autorisations nécessaires à la fonction.

Vous pouvez également utiliser l'opération `AddPermission` dans l'API AWS Lambda pour attacher une stratégie à une fonction. L'appel de l'API `AddPermission` suivant autorise Amazon SES à appeler votre fonction Lambda. Pour en savoir plus sur l'attachement de stratégies à des fonctions Lambda, consultez AWS Lambda Autorisations dans le Guide du développeur AWS Lambda.

```
{
  "Action": "lambda:InvokeFunction",
  "Principal": "ses.amazonaws.com",
  "SourceAccount": "111122223333",
  "SourceArn": "arn:aws:ses:region:111122223333:receipt-rule-set/rule_set_name:receipt-
rule/receipt_rule_name"
  "StatementId": "GiveSESPermissionToInvokeFunction"
}
```

Dans l'exemple précédent, apportez les modifications suivantes :

- Remplacez *region* par la région AWS où vous avez créé la règle de réception.

- Remplacez *111122223333* par votre ID de compte AWS.
- Remplacez *rule_set_name* par le nom du jeu de règles qui contient la règle de réception dans laquelle vous avez créé votre fonction Lambda.
- Remplacez *receipt_rule_name* par le nom de la règle de réception contenant votre fonction Lambda.

Attribuer à Amazon SES l'autorisation de publier dans une rubrique Amazon SNS qui appartient à un autre compte AWS

Si vous souhaitez publier des notifications dans une rubrique d'un compte AWS distinct, vous devez attacher une politique à la rubrique Amazon SNS. La rubrique SNS doit se trouver dans la même région que le jeu de règles de réception et de domaine.

La stratégie suivante autorise Amazon SES à publier dans une rubrique Amazon SNS dans un compte AWS distinct.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":{
        "Service":"ses.amazonaws.com"
      },
      "Action":"SNS:Publish",
      "Resource":"arn:aws:sns:topic_region:sns_topic_account_id:topic_name",
      "Condition":{
        "StringEquals":{
          "AWS:SourceAccount":"aws_account_id",
          "AWS:SourceArn": "arn:aws:ses:receipt_region:aws_account_id:receipt-rule-
set/rule_set_name:receipt-rule/receipt_rule_name"
        }
      }
    }
  ]
}
```

Dans l'exemple précédent, apportez les modifications suivantes :

- Remplacez*topic_region* par le Région AWS dans lequel la rubrique Amazon SNS a été créée.

- Remplacez *sns_topic_account_id* par l'ID du compte AWS qui possède la rubrique Amazon SNS.
- Remplacez *topic_name* par le nom de la rubrique Amazon SNS dans laquelle vous souhaitez publier des notifications.
- Remplacez *aws_account_id* par l'ID du compte AWS qui est configuré pour recevoir des e-mails.
- Remplacez *receipt_region* par la Région AWS où vous avez créé la règle de réception.
- Remplacez *rule_set_name* par le nom du jeu de règles qui contient la règle de réception où vous avez créé votre publication pour l'action de rubrique sur Amazon SNS.
- Remplacez *receipt_rule_name* par le nom de la règle de réception contenant la publication de l'action de la rubrique Amazon SNS.

Si votre rubrique Amazon SNS utilise AWS KMS pour le chiffrement côté serveur, vous devez ajouter des autorisations à la stratégie de clé AWS KMS. Vous pouvez ajouter des autorisations en attachant la stratégie suivante à la stratégie de clé AWS KMS :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSESToUseKMSKey",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

Instructions pour la console de réception d'e-mails Amazon SES

Cette section décrit les assistants de la console de réception des e-mails qui sont utilisés pour configurer les règles de réception et les filtres d'adresses IP afin de gérer la réception de vos e-mails.

Avant d'utiliser les assistants de la console, il est important de lire les deux Concepts de réception d'e-mails et cas d'utilisation pour comprendre les concepts du fonctionnement de la réception des e-mails et Configuration de la réception d'e-mails pour s'assurer que vous avez rempli les conditions préalables à la configuration.

Les assistants de la console permettant de configurer les règles de réception et les filtres d'adresses IP sont expliqués ci-après :

- Création de règles de réception - Démonstration de la console
- Création de filtres d'adresses IP - Démonstration de la console

Création de règles de réception - Démonstration de la console

Cette section vous explique comment créer et définir des règles de réception à l'aide de la console Amazon SES. Les points clés pour comprendre le fonctionnement des règles de réception sont les suivants :

- Jeux de règles contiennent un ensemble ordonné de règles de réception et les règles de réception contiennent un ensemble ordonné d'actions.
- Les règles de réception indiquent à Amazon SES comment traiter l'e-mail entrant en exécutant une liste ordonnée d'actions que vous spécifiez.
- Cette liste ordonnée d'actions peut éventuellement être subordonnée à une condition de destinataire. Si elle n'est pas spécifiée, les actions seront appliquées à toutes les identités qui appartiennent à vos domaines vérifiés.
- Les règles de réception sont créées et définies dans un conteneur appelé jeu de règles. Bien que vous puissiez créer plusieurs jeux de règles, un seul peut être actif à la fois.
- Les règles de réception du jeu de règles actif sont exécutées dans l'ordre que vous avez spécifié.
- Avant de créer vos règles de réception, vous devez d'abord créer un jeu de règles pour les contenir.

Vous pouvez également utiliser l'API `CreateReceiptRuleSet` pour créer un jeu de règles de réception vide, comme décrit dans la référence API Amazon Simple Email Service. Vous pouvez ensuite utiliser la console Amazon SES ou l'API `CreateReceiptRule` pour ajouter des règles de réception dans cet ensemble.

Avant de passer à la démonstration, assurez-vous d'avoir rempli toutes les conditions préalables nécessaires à l'utilisation de la réception d'e-mails basée sur le destinataire. Également

Prérequis

Les conditions préalables suivantes doivent être remplies avant de procéder à la mise en place du contrôle des e-mails basés sur les destinataires à l'aide de règles de réception :

1. Assurez-vous que votre point de terminaison se trouve dans une Région AWS où Amazon SES prend en charge la réception d'e-mails. Consultez Points de terminaison de réception d'e-mails pris en charge par SES.
2. Vous devez d'abord créer et vérifier une identité de domaine dans Amazon SES.
3. Vous devez ensuite indiquer les serveurs de messagerie qui peuvent accepter les e-mails pour votre domaine en publiant un registre MX dans les paramètres DNS de votre domaine. (Le registre MX doit faire référence au point de terminaison Amazon SES qui reçoit l'e-mail pour la région AWS où vous utilisez Amazon SES).
4. Vous devez ensuite donner à Amazon SES l'autorisation d'accéder à d'autres ressources AWS afin d'exécuter les actions de la règle de réception.

Création de jeux de règles et de règles de réception

Cette démonstration commence par la création d'un jeu de règles pour contenir vos règles et se poursuit avec l'assistant de création de règles pour créer, définir et ordonner vos règles de réception. L'assistant contient quatre écrans permettant de définir les paramètres des règles, d'ajouter des conditions relatives aux destinataires, des actions, et de vérifier tous vos paramètres.

Pour créer un jeu de règles et des règles de réception à l'aide de la console

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Email Receiving (Réception d'e-mails).

> **Note**
>
> Réception d'e-mails n'est pas visible dans le volet de navigation gauche de la console SES si votre compte se trouve dans une Région AWS dans laquelle SES ne prend pas en charge la réception d'e-mails. Consultez le premier élément répertorié dans the section called “Prérequis”.

3. Sous l'onglet Receipt rule sets (Jeux de règles de réception) du volet Email receiving (Réception des e-mails), sélectionnez Create rule set (Créer un jeu de règles).
4. Entrez un nom unique pour votre jeu de règles et choisissez Create rule set (Créer un jeu de règles).
5. Choisissez Create rule (Créer une règle), pour ouvrir l'assistant Create rule (Créer une règle).
6. Sur la page Define rule settings (Définir les paramètres de la règle), sous Receipt rule details (Détails de la règle de réception), entrez un nom de règle.
7. Pour Status (État), décochez la case Enabled (Activé) uniquement si vous ne voulez pas qu'Amazon SES exécute cette règle après sa création, sinon, laissez cette option sélectionnée.
8. (Facultatif) Sous Security and protection options (Options de sécurité et de protection), pour protocole TLS (Transport Layer Security), sélectionnez Required (Requis) si vous voulez que Amazon SES rejette les messages entrants qui ne sont pas envoyés via une connexion sécurisée.
9. (Facultatif) Pour Spam and virus scanning (Analyse des spams et des virus), sélectionnez Enabled (Activé) si vous voulez que Amazon SES analyse les messages entrants pour détecter les spams et les virus.
10. Pour passer à l'étape suivante, sélectionnez Next (Suivant).
11. (Facultatif) Sur la page Add recipient conditions (Ajouter les conditions du destinataire), procédez comme suit pour spécifier une ou plusieurs conditions de destinataire. Vous pouvez avoir un maximum de 100 conditions de destinataire par règle de réception.

    a. Sous Recipient conditions (Conditions du destinataire), choisissez Add new recipient condition (Ajouter une nouvelle condition du destinataire) pour spécifier l'e-mail de réception ou le domaine auquel vous voulez appliquer la règle de réception. Le tableau suivant utilise l'adresse utilisateur@exemple.com pour montrer comment spécifier les conditions du destinataire.

Si vous souhaitez...	Spécifier les destinataires suivants...	Remarques
Mettre en correspon dance une adresse e-mail spécifique.	utilisateur@exemple.com	Met également en correspondance les variations de l'adresse qui contiennent des étiquette s (par exemple, utilisateur

Si vous souhaitez...	Spécifier les destinataires suivants...	Remarques
		+123@exemple et utilisateur+xyz@exemple.com). Toutefois, si vous spécifiez une adresse qui contient une étiquette, seule cette adresse spécifique est mise en correspondance.
Mettre en correspondance toutes les adresses au sein d'un domaine, mais pas celles dans ses sous-domaines.	example.com	
Mettre en correspondance les adresses au sein d'un sous-domaine spécifique, mais pas celles dans le domaine parent.	subdomain.example.com	
Mettre en correspondance les adresses au sein de tous les sous-domaines, mais pas celles dans le domaine parent.	.example.com	Notez le point (.) avant le nom de domaine.
Mettre en correspondance toutes les adresses au sein d'un domaine, et tous les adresses de ses sous-domaines.	example.com .example.com	Créez deux destinataires : l'un avec le nom de domaine et l'autre avec un point suivi du nom de domaine.
Mettre en correspondance tous les destinataires dans tous les domaines vérifiés	[Aucune]	Laissez le champ de destinataire vide.

Si vous souhaitez...	Spécifier les destinataires suivants...	Remarques

> **Important**
>
> Si plusieurs comptes Amazon SES reçoivent des e-mails sur un domaine commun (par exemple, si plusieurs équipes de la même société ont chacune des comptes Amazon SES distincts), Amazon SES traite simultanément toutes les règles de réception correspondantes pour chacun de ces comptes. Ce comportement peut entraîner une situation dans laquelle un compte génère un retour à l'expéditeur, tandis qu'un autre compte accepte l'e-mail.
>
> Nous vous recommandons de vous coordonner avec les autres équipes de votre organisation qui utilisent Amazon SES pour vous assurer que chaque compte utilise des règles de réception uniques et que ces règles ne se chevauchent pas. Dans ces situations, il est préférable de configurer vos règles de réception de façon à utiliser uniquement des adresses e-mail ou des sous-domaines qui sont uniques pour votre groupe ou votre équipe.

b. Répétez cette étape pour chaque condition de destinataire que vous souhaitez ajouter. Une fois que vous avez fini d'ajouter les conditions du destinataire, cliquez sur Next (Suivant).

12. Sur la page Add actions (Ajouter des actions), utilisez la procédure suivante pour ajouter une ou plusieurs actions à la règle de réception.

    a. Ouvrez le menu Add new action (Ajouter une nouvelle action), puis choisissez l'un des types d'actions suivants :

    - Ajout d'en-tête - Cette action ajoute un en-tête personnalisé à l'e-mail reçu.
    - Réponse au retour à l'expéditeur - Cette action rejette l'e-mail reçu en renvoyant une réponse de retour à l'expéditeur.
    - Invoquer la fonction Lambda- Cette action appelle votre code via une fonction Lambda AWS.
    - Livrer au compartiment S3 - Cette action stocke l'e-mail reçu dans un compartiment Amazon Simple Storage Service (S3).

- Publie dans une rubrique Amazon SNS. - Cette action publie l'e-mail complet dans une rubrique Amazon Simple Notification Service (SNS).
- Ensemble du jeu de règles - Cette action met fin à l'évaluation du jeu de règles de réception.
- Intégration à Amazon WorkMail - Cette action WorkMail s'intègre à Amazon WorkMail.

Pour en savoir plus sur ces actions, consultez Options d'action.

b. Répétez cette étape pour chaque action que vous souhaitez définir. Si plusieurs actions sont définies, vous pouvez les réorganiser à l'aide des flèches haut/bas dans les conteneurs d'action. Choisissez Next (Suivant) pour passer à la page Review (Vérification).

13. Dans la page Review (Vérification), vérifiez les paramètres et les actions de la règle. Si vous devez apporter des modifications, choisissez l'option Edit (Modifier) ou utilisez la section de navigation sur le côté gauche de la page pour accéder directement à l'étape qui contient le contenu que vous souhaitez modifier. Vous pouvez éventuellement modifier l'ordre des actions énumérées dans le tableau Actions de la page Review (Vérification) en utilisant les flèches haut/bas de la colonne Reorder (Réorganiser).
14. Une fois que vous êtes prêt à continuer, choisissez Create rule (Créer une règle).
15. Sur la page de confirmation du jeu de règles, choisissez Set as active (Définir comme actif) si vous souhaitez appliquer le jeu de règles immédiatement.

Modifications de règle après création

Après avoir créé un jeu de règles, vous pouvez modifier à la fois le jeu de règles et les règles de réception qu'il contient. Elles peuvent non seulement être modifiées, mais il est également possible de dupliquer le jeu de règles ou ses règles afin d'en créer rapidement de nouvelles. La liste suivante présente les modifications disponibles pour le jeu de règles et les règles de réception :

- Rule set (Jeu de règles) est répertorié avec son nom, son statut et sa date de création. Les options de modification du jeu de règles sont les suivantes :
  - Le bouton Set as active/inactive (Définir comme actif/inactif) bascule entre la définition de l'état.
  - Le bouton Duplicate (Dupliquer) copie le jeu de règles. Vous serez invité à fournir un nom unique.
  - Le bouton Delete (Supprimer) permet de supprimer le jeu de règles. Vous serez invité à confirmer cette action irréversible.

- Receipt rules (Règles de réception) sont répertoriés avec leur nom, leur statut, leur sécurité et leur ordre. Les options de modification des règles de réception sont les suivantes :
  - Les Flèches haut/bas permettent réorganiser l'exécution des règles dans l'ensemble de règles.
  - Duplicate (Dupliquer) crée une copie de la règle sélectionnée. Vous serez invité à fournir un nom unique.
  - Le bouton Edit (Modifier) ouvre la règle sélectionnée de sorte que l'un de ses paramètres, tels que les paramètres de la règle, les conditions du destinataire et les actions, puissent être modifiés.
  - Le bouton Delete (Supprimer) permet de supprimer la règle sélectionnée. Vous serez invité à confirmer cette action irréversible.
  - Le bouton Create rule (Créer une règle) permet de créer et d'ajouter une nouvelle règle au jeu de règles en cours.

Options d'action

Chaque règle de réception pour la réception d'e-mails via Amazon SES contient une liste ordonnée d'actions. Cette section décrit les options spécifiques pour chaque type d'action.

Les types d'action sont les suivants :

- Action d'ajout d'en-tête
- Action de réponse au retour à l'expéditeur
- Invoquer l'action de fonction Lambda
- Livrer à l'action du compartiment S3
- Publie dans une action de rubrique Amazon SNS.
- Arrêt de l'action de jeu de règles
- Intégration à l'action Amazon WorkMail

Action d'ajout d'en-tête

L'action Add Header (Ajouter un en-tête) ajoute un en-tête personnalisé à l'e-mail reçu. Vous utilisez généralement cette action uniquement en combinaison avec une autre action. Cette action comporte les options suivantes.

- Header name – Nom de l'en-tête à ajouter. Il doit comporter entre 1 et 50 caractères, inclus, uniquement des caractères alphanumériques (a-z, A-Z, 0-9) et des tirets.

- Header value – Valeur de l'en-tête à ajouter. Celle-ci doit comporter moins de 2048 caractères et ne peut pas contenir de sauts de ligne (« \r » ou « \n »).

Action de réponse au retour à l'expéditeur

L'action Bounce (Retour à l'expéditeur) rejette l'e-mail en renvoyant à l'expéditeur une réponse de retour à l'expéditeur et vous avertit le cas échéant via Amazon SNS. Cette action comporte les options suivantes.

- SMTP Reply Code – Code de réponse SMTP, tel qu'il a été défini par la spécification RFC 5321.
- SMTP Status Code – Code de statut SMTP amélioré, tel qu'il a été défini par la spécification RFC 3463.
- Message – Texte lisible par l'utilisateur à inclure dans l'e-mail de retour à l'expéditeur.
- Reply Sender – Adresse e-mail de l'expéditeur de l'e-mail retourné à l'expéditeur. Il s'agit de l'adresse à partir de laquelle l'e-mail de retour à l'expéditeur sera envoyé. Celle-ci doit être vérifiée avec Amazon SES.
- SNS Topic – Nom ou ARN de la rubrique Amazon SNS pour éventuellement avertir lorsqu'un e-mail de retour à l'expéditeur est envoyé. Voici un exemple d'ARN de rubrique Amazon SNS : arn:aws:sns:us-east-1:123456789012:MyTopic. Vous pouvez également créer une rubrique Amazon SNS lorsque vous configurez une action en choisissant Create SNS Topic (Créer une rubrique SNS). Pour de plus amples informations sur les rubriques Amazon SNS, consultez le guide du développeur d'Amazon Simple Notification Service.

> **Note**
>
> La rubrique Amazon SNS que vous choisissez doit être située dans la même région AWS que le point de terminaison Amazon SES que vous utilisez pour recevoir des e-mails.

Vous pouvez saisir vos propres valeurs pour ces champs, ou choisir un modèle qui remplit les champs SMTP Reply Code, SMTP Status Code et Message avec des valeurs selon la raison du retour à l'expéditeur. Les modèles suivants sont disponibles :

- La boîte de réception n'existe pas – Code de réponse SMTP = 550, code de statut SMTP = 5.1.1
- Message trop grand – Code de réponse SMTP = 552, code de statut SMTP = 5.3.4
- Message plein – Code de réponse SMTP = 552, code de statut SMTP = 5.2.2

- Contenu du message rejeté – Code de réponse SMTP = 500, code de statut SMTP = 5.6.1
- Erreur inconnue – Code de réponse SMTP = 554, code de statut SMTP = 5.0.0
- Échec temporaire – Code de réponse SMTP = 450, code de statut SMTP = 4.0.0

Pour obtenir des codes de retour à l'expéditeur supplémentaires que vous pouvez utiliser en saisissant des valeurs personnalisées dans les champs, consultez la spécification RFC 3463.

Invoquer l'action de fonction Lambda

L'action Lambda appelle votre code via une fonction Lambda et vous avertit éventuellement via Amazon SNS. Cette action a les options et les exigences suivantes.

Options

- Lambda function (Fonction Lambda) — L'ARN de la fonction Lambda. Voici un exemple d'ARN de fonction Lambda : arn:aws:lambda:us-east-1:account-id:function:MyFunction.
- Invocation type (Type d'invocation) — Le type d'appel de la fonction Lambda. Un type d'appel RequestResponse implique que l'exécution de la fonction entraîne une réponse immédiate. Un type d'appel Event (Événement) implique que la fonction est appelée de manière asynchrone. Nous vous conseillons d'utiliser le type d'appel Event (Événement), sauf si une exécution synchrone est absolument nécessaire à votre cas d'utilisation.

  Les appels RequestResponse sont soumis à un délai d'expiration de 30 secondes.

  Pour plus d'informations, veuillez consulter la section Appeler Lambda avec Step Functions dans le Guide du développeur AWS Lambda.
- SNS Topic (Rubrique SNS) — Le nom ou l'ARN de la rubrique Amazon SNS à avertir lorsque la fonction Lambda spécifiée est déclenchée. Voici un exemple d'ARN de rubrique Amazon SNS : arn:aws:sns:us-east-1:123456789012:MyTopic. Pour plus d'informations, consultez Création d'une rubrique Amazon SNS dans le Guide du développeur Amazon Simple Notification Service.

Prérequis

- La fonction Lambda que vous choisissez doit être située dans la même région AWS que le point de terminaison Amazon SES que vous utilisez pour recevoir des e-mails.
- La rubrique Amazon SNS que vous choisissez doit être située dans la même région AWS que le point de terminaison Amazon SES que vous utilisez pour recevoir des e-mails.

Écriture de votre fonction Lambda

Pour traiter les e-mails, votre fonction Lambda peut être appelée de façon asynchrone (c'est-à-dire, à l'aide du type d'appel `Event`). L'objet d'événement transmis à votre fonction Lambda contient des métadonnées concernant l'événement d'e-mail entrant. Vous pouvez également utiliser les métadonnées pour accéder au contenu du message depuis votre compartiment Amazon S3.

Si vous souhaitez réellement contrôler le flux de messagerie, votre fonction Lambda doit être appelée de manière synchrone (c'est-à-dire, à l'aide du type d'appel `RequestResponse`) et votre fonction Lambda doit appeler la méthode `callback` avec deux arguments, le premier argument étant `null` et le deuxième argument, une propriété `disposition` qui est définie sur `STOP_RULE`, `STOP_RULE_SET` ou `CONTINUE`. Si le deuxième argument est `null` ou n'a pas de propriété `disposition` valide, le flux de messagerie continue, et de nouvelles actions et règles sont traitées, ce qui est identique à `CONTINUE`.

Par exemple, vous pouvez arrêter l'ensemble de règles de réception en écrivant la ligne suivante à la fin du code de votre fonction Lambda :

```
callback( null, { "disposition" : "STOP_RULE_SET" });
```

Pour obtenir des exemples de code AWS Lambda, consultez Exemples de fonctions Lambda. Pour obtenir des exemples de cas d'utilisation de haut niveau, consultez Exemples de cas d'utilisation.

Format d'entrée

Amazon SES transmet des informations à la fonction Lambda au format JSON. L'objet de niveau supérieur contient un tableau `Records` qui est alimenté avec les propriétés `eventSource`, `eventVersion` et `ses`. L'objet `ses` contient des objets `receipt` et `mail` qui sont exactement au même format que dans les notifications Amazon SNS décrites dans Contenu des notifications .

Les données qu'Amazon SES transmet à Lambda incluent des métadonnées sur le message, ainsi que plusieurs en-têtes de messagerie. Par contre, elles ne contiennent pas le corps du message.

Voici une vue d'ensemble de la structure de l'entrée fournie par Amazon SES à la fonction Lambda.

```
{
   "Records": [
      {
        "eventSource": "aws:ses",
        "eventVersion": "1.0",
```

```
        "ses": {
           "receipt": {
               <same contents as SNS notification>
            },
           "mail": {
               <same contents as SNS notification>
           }
         }
     }
   ]
}
```

Valeurs de retour

Votre fonction Lambda peut contrôler le flux de messagerie en renvoyant l'une des valeurs suivantes :

- `STOP_RULE` – Aucune autre action de la règle de réception actuelle ne sera traitée, mais d'autres règles de réception peuvent être traitées.
- `STOP_RULE_SET` – Aucune autre action ou règle de réception ne sera traitée.
- `CONTINUE` (ou toute autre valeur non valide) – Signifie que de nouvelles actions et règles de réception peuvent être traitées.

Les rubriques suivantes couvrent des exemples d'événements de messagerie entrants, des exemples de cas d'utilisation de haut niveau et exemples de code AWS Lambda :

- Exemples de cas d'utilisation
- Exemples de fonctions Lambda

Exemples de cas d'utilisation

Les exemples suivants décrivent certaines règles que vous pouvez configurer pour utiliser les résultats d'une fonction Lambda afin de contrôler votre flux de messagerie. À des fins de démonstration, de nombreux exemples utilisent l'action S3 comme le résultat.

Cas d'utilisation 1 : Supprimer le courrier indésirable pour tous les domaines

Cet exemple illustre une règle globale qui supprime le courrier indésirable dans l'ensemble de vos domaines. Les règles 2 et 3 sont incluses pour montrer que vous pouvez appliquer des règles spécifiques au domaine une fois le courrier indésirable supprimé dans tous les domaines.

Règle 1

Liste des destinataires : Vide. Cette règle s'applique donc à tous les destinataires sous tous vos domaines vérifiés.

Actions

1. Action Lambda (synchrone) qui renvoie `STOP_RULE_SET` si l'e-mail est un courrier indésirable. Sinon, la valeur renvoyée est `CONTINUE`. Consultez l'exemple de fonction Lambda pour la suppression du courrier indésirable dans Exemples de fonctions Lambda.

Règle 2

Liste des destinataires : exemple1.com

Actions

1. Toute action.

Règle 3

Liste des destinataires : exemple2.com

Actions

1. Toute action.

Cas d'utilisation 2 : Retourner à l'expéditeur le courrier indésirable pour tous les domaines

Cet exemple illustre une règle globale qui retourne à l'expéditeur le courrier indésirable pour l'ensemble de vos domaines. Les règles 2 et 3 sont incluses pour montrer que vous pouvez appliquer des règles spécifiques au domaine une fois le courrier indésirable renvoyé à l'expéditeur pour tous les domaines.

Règle 1

Liste des destinataires : Vide. Cette règle s'applique donc à tous les destinataires sous tous vos domaines vérifiés.

Actions

1. Action Lambda (synchrone) qui renvoie `CONTINUE` si l'e-mail est un courrier indésirable. Sinon, la valeur renvoyée est `STOP_RULE`.
2. Action de retour à l'expéditeur (« 500 5.6.1. Contenu du message rejeté »).
3. Action d'arrêt.

Règle 2

Liste des destinataires : exemple1.com

Actions

1. Toute action

Règle 3

Liste des destinataires : exemple2.com

Actions

1. Toute action

Cas d'utilisation 3 : Appliquer la règle la plus spécifique

Cet exemple montre comment utiliser l'action d'arrêt pour empêcher que des e-mails soient traités par plusieurs règles. Dans cet exemple, vous disposez d'une règle pour une adresse spécifique et d'une autre règle pour toutes les adresses e-mail sous le domaine. En utilisant l'action d'arrêt, vous faites en sorte que les messages qui correspondent à la règle pour l'adresse e-mail spécifique ne soient pas traités par la règle plus générique qui s'applique au domaine.

Règle 1

Liste des destinataires : utilisateur@exemple.com

Actions

1. Action Lambda (asynchrone).
2. Action d'arrêt.

Règle 2

Liste des destinataires : exemple.com

Actions

1. Toute action.

Cas d'utilisation 4 : Consigner les événements de messagerie dans CloudWatch

Cet exemple montre comment conserver un journal d'audit de tous les messages transitant par votre système avant d'enregistrer les messages dans Amazon SES.

Règle 1

Liste des destinataires : exemple.com

Actions

1. Action Lambda (asynchrone) qui écrit l'objet d'événement dans un journal CloudWatch. Les exemples de fonctions Lambda de Exemples de fonctions Lambda journalisent dans CloudWatch.
2. Action S3.

Cas d'Application 5 : Supprimer les messages pour lesquels le contrôle DKIM échoue

Cet exemple montre comment enregistrer tous les messages entrants dans un compartiment Amazon S3, mais envoyer uniquement les e-mails destinés à une adresse e-mail spécifique et pour lesquels le contrôle DKIM réussit à votre application de messagerie automatisée.

Règle 1

Liste des destinataires : exemple.com

Actions

1. Action S3.
2. Action Lambda (synchrone) qui renvoie `STOP_RULE_SET` si le contrôle DKIM échoue pour le message. Sinon, la valeur renvoyée est `CONTINUE`.

Règle 2

Liste des destinataires : support@exemple.com

Actions

1. Action Lambda (asynchrone) qui déclenche l'application automatisée.

Cas d'application 6 : Filtrer les messages en fonction de l'objet

Cet exemple montre comment supprimer tous les messages entrants d'un domaine contenant le mot « remise » dans l'objet, puis traiter les messages destinés à un système automatisé d'une façon et traiter les e-mails adressée à tous les autres destinataires du domaine de manière différente.

Règle 1

Liste des destinataires : exemple.com

Actions

1. Action Lambda (synchrone) qui renvoie `STOP_RULE_SET` si l'objet contient le mot « remise ». Sinon, la valeur renvoyée est `CONTINUE`.

Règle 2

Liste des destinataires : support@exemple.com

Actions

1. Action S3 avec le compartiment 1.
2. Action Lambda (asynchrone) qui déclenche l'application automatisée.
3. Action d'arrêt.

Règle 3

Liste des destinataires : exemple.com

Actions

1. Action S3 avec le compartiment 2.
2. Action Lambda (asynchrone) qui traite les e-mails pour le reste du domaine.

Exemples de fonctions Lambda

Cette rubrique contient des exemples de fonctions Lambda qui contrôlent le flux de messagerie.

Exemple 1 : Suppression du courrier indésirable

Cet exemple arrête de traiter les messages qui ont au moins un indicateur de courrier indésirable.

```
exports.handler = function(event, context, callback) {
    console.log('Spam filter');

    var sesNotification = event.Records[0].ses;
    console.log("SES Notification:\n", JSON.stringify(sesNotification, null, 2));

    // Check if any spam check failed
    if (sesNotification.receipt.spfVerdict.status === 'FAIL'
            || sesNotification.receipt.dkimVerdict.status === 'FAIL'
            || sesNotification.receipt.spamVerdict.status === 'FAIL'
            || sesNotification.receipt.virusVerdict.status === 'FAIL') {
        console.log('Dropping spam');
        // Stop processing rule set, dropping message
        callback(null, {'disposition':'STOP_RULE_SET'});
    } else {
        callback(null, null);
    }
};
```

Exemple 2 : Continuer si un en-tête spécifique est trouvé

Cet exemple continue de traiter la règle actuelle uniquement si l'e-mail contient une valeur d'en-tête spécifique.

```
exports.handler = function(event, context, callback) {
    console.log('Header matcher');

    var sesNotification = event.Records[0].ses;
    console.log("SES Notification:\n", JSON.stringify(sesNotification, null, 2));

    // Iterate over the headers
    for (var index in sesNotification.mail.headers) {
        var header = sesNotification.mail.headers[index];

        // Examine the header values
        if (header.name === 'X-Header' && header.value === 'X-Value') {
```

```
            console.log('Found header with value.');
            callback(null, null);
            return;
        }
    }

    // Stop processing the rule if the header value wasn't found
    callback(null, {'disposition':'STOP_RULE'});
};
```

Exemple 3 : Récupération de l'e-mail depuis Amazon S3

Cet exemple extrait l'e-mail brut d'Amazon S3 et le traite.

> **Note**
>
> Vous devez d'abord écrire l'e-mail dans Amazon S3 à l'aide d'une action S3.

```
var AWS = require('aws-sdk');
var s3 = new AWS.S3();

var bucketName = '<YOUR BUCKET GOES HERE>';

exports.handler = function(event, context, callback) {
    console.log('Process email');

    var sesNotification = event.Records[0].ses;
    console.log("SES Notification:\n", JSON.stringify(sesNotification, null, 2));

    // Retrieve the email from your bucket
    s3.getObject({
            Bucket: bucketName,
            Key: sesNotification.mail.messageId
        }, function(err, data) {
            if (err) {
                console.log(err, err.stack);
                callback(err);
            } else {
                console.log("Raw email:\n" + data.Body);

                // Custom email processing goes here
```

```
                callback(null, null);
            }
        });
};
```

Exemple 4 : Retour à l'expéditeur des messages pour lesquels l'authentification DMARC échoue

Cet exemple envoie un message de retour à l'expéditeur si l'authentification DMARC échoue pour des e-mails entrants.

> **Note**
>
> Lorsque vous utilisez cet exemple, définissez la valeur de la variable d'environnement `emailDomain` sur votre domaine de réception des e-mails.

```
'use strict';

const AWS = require('aws-sdk');

// Assign the emailDomain environment variable to a constant.
const emailDomain = process.env.emailDomain;

exports.handler = (event, context, callback) => {
    console.log('Spam filter starting');

    const sesNotification = event.Records[0].ses;
    const messageId = sesNotification.mail.messageId;
    const receipt = sesNotification.receipt;

    console.log('Processing message:', messageId);

    // If DMARC verdict is FAIL and the sending domain's policy is REJECT
    // (p=reject), bounce the email.
    if (receipt.dmarcVerdict.status === 'FAIL'
        && receipt.dmarcPolicy.status === 'REJECT') {
        // The values that make up the body of the bounce message.
        const sendBounceParams = {
            BounceSender: `mailer-daemon@${emailDomain}`,
            OriginalMessageId: messageId,
            MessageDsn: {
                ReportingMta: `dns; ${emailDomain}`,
```

```
                ArrivalDate: new Date(),
                ExtensionFields: [],
            },
            // Include custom text explaining why the email was bounced.
            Explanation: "Unauthenticated email is not accepted due to the sending
 domain's DMARC policy.",
            BouncedRecipientInfoList: receipt.recipients.map((recipient) => ({
                Recipient: recipient,
                // Bounce with 550 5.6.1 Message content rejected
                BounceType: 'ContentRejected',
            })),
        };

        console.log('Bouncing message with parameters:');
        console.log(JSON.stringify(sendBounceParams, null, 2));
        // Try to send the bounce.
        new AWS.SES().sendBounce(sendBounceParams, (err, data) => {
            // If something goes wrong, log the issue.
            if (err) {
                console.log(`An error occurred while sending bounce for message:
 ${messageId}`, err);
                callback(err);
            // Otherwise, log the message ID for the bounce email.
            } else {
                console.log(`Bounce for message ${messageId} sent, bounce message ID:
 ${data.MessageId}`);
                // Stop processing additional receipt rules in the rule set.
                callback(null, {
                    disposition: 'stop_rule_set',
                });
            }
        });
    // If the DMARC verdict is anything else (PASS, QUARANTINE or GRAY), accept
    // the message and process remaining receipt rules in the rule set.
    } else {
        console.log('Accepting message:', messageId);
        callback();
    }
};
```

Livrer à l'action du compartiment S3

L'action S3 remet les messages dans un compartiment Amazon S3 et vous avertit éventuellement via Amazon SNS. Cette action comporte les options suivantes.

- S3 Bucket – Nom du compartiment Amazon S3 dans lequel enregistrer les e-mails reçus. Vous pouvez également créer un nouveau compartiment Amazon S3 lorsque vous configurez une action en choisissant Create S3 Bucket (Créer un compartiment S3). Amazon SES vous fournit l'e-mail brut non modifié, généralement au format Multipurpose Internet Mail Extensions (MIME). Pour plus de détails sur le format MIME, consultez la spécification RFC 2045.

  > **Important**
  >
  > - Lorsque vous enregistrez vos messages dans compartiment Amazon S3, la taille maximale par défaut des e-mails est de 40 Mo, en-têtes compris.
  > - SES ne prend pas en charge les règles de réception qui chargent vers S3 des compartiments avec le verrouillage d'objets activé et configuré avec une période de rétention par défaut.
  > - Si vous appliquez le chiffrement à votre compartiment S3 en spécifiant votre propre clé KMS, veillez à utiliser l'ARN de clé KMS complet, et non l'alias de clé KMS. L'utilisation de l'alias peut entraîner le chiffrement des données avec une clé KMS appartenant au demandeur, et non à l'administrateur du compartiment. Veuillez consulter Utilisation du chiffrement pour les opérations inter-comptes.
  > - SES ne prend pas en charge les compartiments S3 dans les régions d'adhésion en tant que destination des e-mails entrants.

- Object Key Prefix – Préfixe de nom de clé à utiliser dans le compartiment Amazon S3. Les préfixes de nom de clé vous permettent d'organiser votre compartiment Amazon S3 dans une structure de dossiers. Par exemple, si vous utilisez E-mail pour Object Key Prefix (Préfixe de clé d'objet), vos e-mails apparaîtront dans votre compartiment Amazon S3 dans un dossier nommé E-mail.
- Clé KMS, si Encrypt Message (Chiffrer le message) est sélectionné dans la console Amazon SES - La clé KMS AWS que Amazon SES doit utiliser pour chiffrer vos e-mails avant de les enregistrer dans le compartiment Amazon S3. Vous pouvez utiliser la clé principale par défaut ou une clé principale personnalisée que vous avez créée dans AWS KMS.

> **Note**
>
> La clé KMS que vous choisissez doit être située dans la même région AWS que le point de terminaison Amazon SES que vous utilisez pour recevoir des e-mails.

- Pour utiliser la clé KMS par défaut, choisissez aws/ses lorsque vous configurez la règle de réception dans la console Amazon SES. Si vous utilisez l'API Amazon SES, vous pouvez spécifier la clé KMS par défaut en fournissant un ARN au format `arn:aws:kms:REGION:AWSACCOUNTID:alias/aws/ses`. Par exemple, si votre ID de compte AWS est 123456789012 et que vous souhaitez utiliser la clé KMS par défaut dans la région us-east-1, l'ARN de la clé KMS par défaut est `arn:aws:kms:us-east-1:123456789012:alias/aws/ses`. Si vous utilisez la clé KMS par défaut, vous n'avez pas besoin d'effectuer des étapes supplémentaires pour autoriser Amazon SES à utiliser la clé.
- Pour utiliser une clé gérée personnalisée que vous avez créée dans AWS KMS, fournissez l'ARN de celle-ci et veillez à ajouter une déclaration à la stratégie de votre clé pour autoriser Amazon SES à l'utiliser. Pour en savoir plus sur l'octroi d'autorisations, consultez Attribution d'autorisations à Amazon SES pour la réception d'e-mails.

Pour en savoir plus sur l'utilisation d'AWS KMS avec Amazon SES, consultez le guide du développeur AWS Key Management Service. Si vous ne spécifiez pas de clé KMS dans la console ou l'API, Amazon SES ne chiffre pas vos e-mails.

> **Important**
>
> Vos messages sont chiffrés par Amazon SES à l'aide du client de chiffrement Amazon S3 avant qu'ils soient envoyés dans Amazon S3 pour stockage. Ils ne sont pas chiffrés à l'aide du chiffrement côté serveur Amazon S3. Cela signifie que vous devez utiliser le client de chiffrement Amazon S3 pour déchiffrer les e-mails après les avoir récupérés depuis Amazon S3, car le service n'a pas accès à vos clés AWS KMS pour le déchiffrement. Ce client de chiffrement est disponible dans le kit AWS SDK for Java et le kit AWS SDK for Ruby. Pour en savoir plus, veuillez consulter Guide de l'utilisateur Amazon Simple Storage Service.

- SNS Topic – Nom ou ARN de la rubrique Amazon SNS à avertir lorsqu'un e-mail est enregistré dans le compartiment Amazon S3. Voici un exemple d'ARN de rubrique Amazon SNS :

arn:aws:sns:us-east-1:123456789012:MyTopic. Vous pouvez également créer une rubrique Amazon SNS lorsque vous configurez une action en choisissant Create SNS Topic (Créer une rubrique SNS). Pour de plus amples informations sur les rubriques Amazon SNS, consultez le guide du développeur d'Amazon Simple Notification Service.

> **Note**
>
> La rubrique Amazon SNS que vous choisissez doit être située dans la même région AWS que le point de terminaison Amazon SES que vous utilisez pour recevoir des e-mails.

Publie dans une action de rubrique Amazon SNS.

L'action SNS publie les messages à l'aide d'une notification Amazon SNS. La notification comprend la totalité du contenu de l'e-mail. Cette action comporte les options suivantes.

- SNS Topic – Nom ou ARN de la rubrique Amazon SNS dans laquelle vous voulez publier les e-mails. Les notifications Amazon SNS contiennent une copie brute non modifiée de l'e-mail, qui est généralement au format Multipurpose Internet Mail Extensions (MIME). Pour plus de détails sur le format MIME, consultez la spécification RFC 2045.

  > **Important**
  >
  > Si vous décidez de recevoir vos messages via des notifications Amazon SNS, la taille maximale des e-mails est de 150 Ko, en-têtes compris. Les e-mails plus volumineux seront renvoyés à l'expéditeur. Si vous prévoyez de recevoir des e-mails d'une taille supérieure, enregistrez-les plutôt dans un compartiment Amazon S3.

  Voici un exemple d'ARN de rubrique Amazon SNS : arn:aws:sns:us-east-1:123456789012:MyTopic. Vous pouvez également créer une rubrique Amazon SNS lorsque vous configurez une action en choisissant Create SNS Topic (Créer une rubrique SNS). Pour de plus amples informations sur les rubriques Amazon SNS, consultez le guide du développeur d'Amazon Simple Notification Service.

> **Note**
>
> La rubrique Amazon SNS que vous choisissez doit être située dans la même région AWS que le point de terminaison Amazon SES que vous utilisez pour recevoir des e-mails.

- Encoding – Encodage à utiliser pour l'e-mail dans la notification Amazon SNS. UTF-8 est plus facile à utiliser, mais risque de ne pas conserver tous les caractères spéciaux lorsqu'un message a été codé avec un format d'encodage différent. Base64 conserve tous les caractères spéciaux. Pour en savoir plus sur UTF-8 et Base64, consultez les spécifications RFC 3629 et RFC 4648, respectivement.

Lorsque vous recevez un e-mail, Amazon SES exécute les règles dans le jeu de règles de réception actif. Vous pouvez configurer des règles de réception de façon à recevoir des notifications à l'aide d'Amazon SNS. Vos règles de réception peuvent envoyer deux types de notifications différents :

- Notifications envoyées par les actions SNS - Lorsque vous ajoutez une action SNS à une règle de réception, elle envoie des informations sur l'e-mail ainsi que sur son contenu. Si le message fait 150 Ko ou moins, ce type de notification comprend également le corps MIME complet de l'e-mail.
- Notifications envoyées à partir d'autres types d'actions – Lorsque vous ajoutez un autre type d'action (dont les actions Bounce (Retour à l'expéditeur), Lambda, Stop Rule Set (Arrêter l'ensemble de règles), ou WorkMail) à une règle de réception, vous pouvez spécifier une rubrique Amazon SNS si vous le souhaitez. Le cas échéant, vous recevrez des notifications lors de l'exécution de ces actions. Ces notifications comportent des informations sur l'e-mail, mais pas sur son contenu.

Les rubriques suivantes décrivent le contenu de ces notifications et fournissent un exemple de chaque type de notification :

- Contenu des notifications pour la réception d'e-mails via Amazon SES
- Exemples de notifications pour la réception d'e-mails via Amazon SES

Contenu des notifications pour la réception d'e-mails via Amazon SES

Toutes les notifications pour la réception d'e-mails sont publiées dans des rubriques Amazon Simple Notification Service (Amazon SNS) au format JavaScript Objet Notation (JSON).

Pour des exemples de notifications, consultez Exemples de notification .

Table des matières

Objet JSON de niveau supérieur

L'objet JSON de niveau supérieur contient les champs suivants.

Nom de champ	Description
`notificationType`	Type de notification. Pour ce type de notification, la valeur est toujours `Received`.
`receipt`	Objet qui contient des informations sur la remise de l'e-mail.
`mail`	Objet qui contient des informations sur l'e-mail auquel la notification est associée.
`content`	Chaîne qui contient l'e-mail brut non modifié, généralement au format Multipurpose Internet Mail Extensions (MIME). Pour plus de détails sur le format MIME, consultez la spécification RFC 2045.

Nom de champ	Description
	Note Ce champ est disponible uniquement si la notification a été déclenchée par une action SNS. Les notifications déclenché es par toutes les autres actions ne contiennent pas ce champ.

Objet receipt

L'objet `receipt` comporte les champs suivants.

Nom de champ	Description
`action`	Objet qui encapsule des informations sur l'action qui a été exécutée. Pour obtenir une liste des valeurs possibles, consultez Objets action.
`dkimVerdict`	Objet qui indique si le contrôle DKIM (DomainKeys Identified Mail) a réussi. Pour obtenir une liste des valeurs possibles, consultez Objet dkimVerdict.
`dmarcPolicy`	Indique les paramètres DMARC (Domain-b ased Message Authentication, Reporting and Conformance) pour le domaine d'envoi. Ce champ apparaît uniquement si le message échoue à l'authentification DMARC. Les valeurs possibles pour ce champ sont les suivantes : • `none` : Le propriétaire du domaine d'envoi demande qu'aucune action spécifique ne soit

Nom de champ	Description
	exécutée sur les messages pour lesquels l'authentification DMARC échoue. • `quarantine` : Le propriétaire du domaine d'envoi demande que les messages pour lesquels l'authentification DMARC échoue soit traités comme étant suspects par les serveurs de messagerie. • `reject` : Le propriétaire du domaine d'envoi demande que les messages pour lesquels l'authentification DMARC échoue soient rejetés.
`dmarcVerdict`	Objet qui indique si le contrôle DMARC (Domain-based Message Authentication, Reporting and Conformance) a réussi. Pour obtenir une liste des valeurs possibles, consultez Objet dmarcVerdict.
`processingTimeMillis`	Chaîne qui spécifie le délai, en milliseco ndes, entre le moment où Amazon SES reçoit le message et le moment où l'action est déclenchée.
`recipients`	Une liste des destinataires (plus particuli èrement les adresses RCPT TO de l'envelop pe) qui ont été retrouvés par la règle de réception active. Les adresses répertoriées ici peuvent être différentes de celles figurant dans le champ `destination` de l'objet the section called “Objet mail”.
`spamVerdict`	Objet qui indique si le message est un courrier indésirable. Pour obtenir une liste des valeurs possibles, consultez Objet spamVerdict.

Nom de champ	Description
`spfVerdict`	Objet qui indique si le contrôle SPF (Sender Policy Framework) a réussi. Pour obtenir une liste des valeurs possibles, consultez Objet spfVerdict.
`timestamp`	Chaîne qui spécifie la date et l'heure qualifiées auxquelles l'action a été déclenchée, au format ISO 8601.
virusVerdict	Objet qui indique si le message contient un virus. Pour obtenir une liste des valeurs possibles, consultez Objet virusVerdict.

Objets action

L'objet `action` comporte les champs suivants.

Nom de champ	Description
`type`	Chaîne qui indique le type d'action exécuté. Les valeurs possibles sont `S3`, `SNS`, `Bounce`, `Lambda`, `Stop` et `WorkMail`.
`topicArn`	Chaîne qui contient l'ARN (Amazon Resource Name) de la rubrique Amazon SNS où la notification a été publiée.
`bucketName`	Chaîne qui contient le nom du compartiment Amazon S3 où la notification a été publiée. Présente uniquement pour le type d'action S3.
`objectKey`	Chaîne qui contient un nom qui identifie l'e-mail dans le compartiment Amazon S3. Cette chaîne est identique à `messageId` dans l'objet the section called “Objet mail”. Présente uniquement pour le type d'action S3.

Nom de champ	Description
`smtpReplyCode`	Chaîne qui contient le code de réponse SMTP, tel qu'il a été défini par la spécification RFC 5321. Présente uniquement pour le type de retour à l'expéditeur.
`statusCode`	Chaîne qui contient le code de statut SMTP amélioré, tel qu'il a été défini par la spécification RFC 3463. Présente uniquement pour le type de retour à l'expéditeur.
`message`	Chaîne qui contient le texte lisible par l'utilisa teur à inclure dans le message de retour à l'expéditeur. Présente uniquement pour le type de retour à l'expéditeur.
`sender`	Chaîne qui contient l'adresse e-mail de l'expédit eur de l'e-mail renvoyé à l'expéditeur. Il s'agit de l'adresse à partir de laquelle le message de retour à l'expéditeur a été envoyé. Présente uniquement pour le type de retour à l'expédit eur.
`functionArn`	Chaîne qui contient l'ARN de la fonction Lambda qui a été déclenchée. Présente uniquement pour le type d'action Lambda.
`invocationType`	Chaîne qui contient le type d'appel de la fonction Lambda. Les valeurs possibles sont `RequestResponse` et `Event`. Présente uniquement pour le type d'action Lambda.
`organizationArn`	Chaîne qui contient l'ARN de l'organisation Amazon WorkMail. Présente uniquement pour le type d'action WorkMail.

Objet dkimVerdict

L'objet `dkimVerdict` comporte les champs suivants.

Nom de champ	Description
`status`	Chaîne qui contient le résultat du contrôle DKIM. Les valeurs possibles sont : • `PASS` : Authentification DKIM réussie pour le message. • `FAIL` : Échec de l'authentification DKIM pour le message. • `GRAY` : le message n'est pas signé par DKIM ou le domaine d'origine et le domaine de signature DKIM ne correspondent pas. • `PROCESSING_FAILED` : Un problème empêche Amazon SES de vérifier la signature DKIM. Par exemple, des requêtes DNS sont défaillantes ou l'en-tête de signature DKIM n'est pas formaté correctem ent.

Objet dmarcVerdict

L'objet `dmarcVerdict` comporte les champs suivants.

Nom de champ	Description
`status`	Chaîne qui contient le résultat du contrôle DMARC. Les valeurs possibles sont : • `PASS` : L'authentification DMARC a réussi pour le message. • `FAIL` : L'authentification DMARC a échoué pour le message.

Nom de champ	Description
	• `GRAY` : au moins une authentification SPF ou DKIM a passé l'authentification, mais le domaine d'envoi ne dispose pas d'une politique DMARC ou utilise la politique `p=none`. • `PROCESSING_FAILED` : Un problème empêche Amazon SES de fournir le résultat d'une authentification DMARC.

Objet spamVerdict

L'objet `spamVerdict` comporte les champs suivants.

Nom de champ	Description
`status`	Chaîne qui contient le résultat de la recherche de courrier indésirable. Les valeurs possibles sont : • `PASS` : l'analyse du courrier indésirable a déterminé qu'il était peu probable que le message contienne un courrier indésirable. • `FAIL` : l'analyse du courrier indésirable a déterminé qu'il était probable que le message contienne un courrier indésirable. • `GRAY` : Amazon SES a analysé l'e-mail mais n'a pas pu déterminer avec fiabilité s'il s'agit d'un courrier indésirable. • `PROCESSING_FAILED` : Amazon SES n'a pas pu analyser l'e-mail. Par exemple, l'e-mail n'est pas un message MIME valide.

Objet spfVerdict

L'objet `spfVerdict` comporte les champs suivants.

Nom de champ	Description
`status`	Chaîne qui contient le résultat du contrôle SPF. Les valeurs possibles sont : • `PASS` : Authentification SPF réussie pour le message. • `FAIL` : Échec de l'authentification SPF pour le message. • `GRAY` : Le résultat SPF est `none`, `softfail` ou `neutral`. • `PROCESSING_FAILED` : Un problème empêche Amazon SES de vérifier le registre SPF. Par exemple, des requêtes DNS échouent.

Objet virusVerdict

L'objet `virusVerdict` comporte les champs suivants.

Nom de champ	Description
`status`	Chaîne qui contient le résultat de la recherche de virus. Les valeurs possibles sont : • `PASS` : Le message ne contient pas de virus. • `FAIL` : Le message contient un virus. • `GRAY` : Amazon SES a analysé l'e-mail mais n'a pas pu déterminer avec fiabilité s'il contient un virus. • `PROCESSING_FAILED` : Amazon SES n'est pas en mesure d'analyser le contenu de

Nom de champ	Description
	l'e-mail. Par exemple, l'e-mail n'est pas un message MIME valide.

Objet mail

L'objet `mail` comporte les champs suivants.

Nom de champ	Description
`destination`	Une liste complète de toutes les adresses de destination (y compris des destinataires A : et Cc :) depuis les en-têtes MIME des e-mails entrants.
`messageId`	Chaîne qui contient l'ID unique attribué à l'e-mail par Amazon SES. Si l'e-mail a été remis à Amazon S3, l'ID de message est également la clé d'objet Amazon S3 qui a été utilisée pour écrire le message dans votre compartiment Amazon S3.
`source`	Chaîne qui contient l'adresse e-mail (plus spécifiquement l'adresse MAIL FROM de l'enveloppe) à partir de laquelle le message a été envoyé.
`timestamp`	Chaîne qui contient la date et l'heure auxquelle s l'e-mail a été reçu, au format ISO8601.
`headers`	Les en-têtes Amazon SES et vos en-têtes personnalisés. Chaque en-tête possède les champs suivants : `name` et `value`.
`commonHeaders`	Les en-têtes communs à tous les e-mails. Chaque en-tête possède les champs suivants : `name` et `value`.

Nom de champ	Description
`headersTruncated`	Spécifie si les en-têtes ont été tronqués dans la notification, ce qui a lieu si les en-têtes ont une taille supérieure à 10 Ko. Les valeurs possibles sont `true` et `false`.

Objet commonHeaders

L'objet `commonHeaders` peut avoir les champs illustrés dans le tableau suivant. Les champs présents dans cet objet varient selon les champs qui étaient présents dans les e-mails entrants.

Nom de champ	Description
`messageId`	ID du message original.
`date`	Date et heure auxquelles Amazon SES a reçu le message.
`to`	L'en-tête To de l'e-mail.
`cc`	L'en-tête CC de l'e-mail.
`bcc`	L'en-tête BCC de l'e-mail.
`from`	L'en-tête From de l'e-mail.
`sender`	L'en-tête Sender de l'e-mail.
`returnPath`	L'en-tête Return-Path de l'e-mail.
`replyTo`	L'en-tête Reply-To de l'e-mail.
`subject`	L'en-tête Subject de l'e-mail.

Exemples de notifications pour la réception d'e-mails via Amazon SES

Cette section inclut des exemples des trois types de notification suivants :

- Une notification envoyée comme résultat d'une action SNS.
- Une notification envoyée à la suite d'un autre type d'action (une notification d'alerte).

Notification d'une action SNS

Cette section contient un exemple d'une notification d'action SNS. Contrairement à la notification d'alerte illustrée précédemment, cette notification inclut une section `content` contenant l'e-mail, généralement au format Multipurpose Internet Mail Extensions (MIME).


```
{
  "notificationType":"Received",
  "receipt":{
    "timestamp":"2015-09-11T20:32:33.936Z",
    "processingTimeMillis":222,
    "recipients":[
      "recipient@example.com"
    ],
    "spamVerdict":{
      "status":"PASS"
    },
    "virusVerdict":{
      "status":"PASS"
    },
    "spfVerdict":{
      "status":"PASS"
    },
    "dkimVerdict":{
      "status":"PASS"
    },
    "action":{
      "type":"SNS",
      "topicArn":"arn:aws:sns:us-east-1:012345678912:example-topic"
    }
  },
  "mail":{
    "timestamp":"2015-09-11T20:32:33.936Z",
    "source":"61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com",
    "messageId":"d6iitobk75ur44p8kdnnp7g2n800",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
```

```
    "headers":[
      {
        "name":"Return-Path",

 "value":"<0000014fbe1c09cf-7cb9f704-7531-4e53-89a1-5fa9744f5eb6-000000@amazonses.com>"
      },
      {
        "name":"Received",
        "value":"from a9-183.smtp-out.amazonses.com (a9-183.smtp-out.amazonses.com
 [54.240.9.183]) by inbound-smtp.us-east-1.amazonaws.com with SMTP id
 d6iitobk75ur44p8kdnnp7g2n800 for recipient@example.com; Fri, 11 Sep 2015 20:32:33
 +0000 (UTC)"
      },
      {
        "name":"DKIM-Signature",
        "value":"v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple;
 s=ug7nbtf4gccmlpwj322ax3p6ow6yfsug; d=amazonses.com; t=1442003552;
 h=From:To:Subject:MIME-Version:Content-Type:Content-Transfer-Encoding:Date:Message-
ID:Feedback-ID; bh=DWr3IOmYWoXCA9ARqGC/UaODfghffiwFNRIb2Mckyt4=;
 b=p4ukUDSFqhqiub+zPR0DW1kp7oJZakrzupr6LBe6sUuvqpBkig56UzUwc29rFbJF
 hlX3Ov7DeYVNoN38stqwsF8ivcajXpQsXRC1cW9z8x875J041rClAjV7EGbLmudVpPX
 4hHst1XPyX5wmgdHIhmUuh8oZKpVqGi6bHGzzf7g="
      },
      {
        "name":"From",
        "value":"sender@example.com"
      },
      {
        "name":"To",
        "value":"recipient@example.com"
      },
      {
        "name":"Subject",
        "value":"Example subject"
      },
      {
        "name":"MIME-Version",
        "value":"1.0"
      },
      {
        "name":"Content-Type",
        "value":"text/plain; charset=UTF-8"
      },
      {
```

```
        "name":"Content-Transfer-Encoding",
        "value":"7bit"
      },
      {
        "name":"Date",
        "value":"Fri, 11 Sep 2015 20:32:32 +0000"
      },
      {
        "name":"Message-ID",
        "value":"<61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>"
      },
      {
        "name":"X-SES-Outgoing",
        "value":"2015.09.11-54.240.9.183"
      },
      {
        "name":"Feedback-ID",
        "value":"1.us-east-1.Krv2FKpFdWV+KUYw3Qd6wcpPJ4Sv/pOPpEPSHn2u2o4=:AmazonSES"
      }
    ],
    "commonHeaders":{

 "returnPath":"0000014fbe1c09cf-7cb9f704-7531-4e53-89a1-5fa9744f5eb6-000000@amazonses.com",
      "from":[
        "sender@example.com"
      ],
      "date":"Fri, 11 Sep 2015 20:32:32 +0000",
      "to":[
        "recipient@example.com"
      ],
      "messageId":"<61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>",
      "subject":"Example subject"
    }
  },
  "content":"Return-Path: <61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>\r
\nReceived: from a9-183.smtp-out.amazonses.com (a9-183.smtp-out.amazonses.com
 [54.240.9.183])\r\n by inbound-smtp.us-east-1.amazonaws.com with SMTP id
 d6iitobk75ur44p8kdnnp7g2n800\r\n for recipient@example.com;\r\n Fri, 11 Sep 2015
 20:32:33 +0000 (UTC)\r\nDKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/
simple;\r\n\ts=ug7nbtf4gccmlpwj322ax3p6ow6yfsug; d=amazonses.com; t=1442003552;\r\n
\th=From:To:Subject:MIME-Version:Content-Type:Content-Transfer-Encoding:Date:Message-
ID:Feedback-ID;\r\n\tbh=DWr3IOmYWoXCA9ARqGC/UaODfghffiwFNRIb2Mckyt4=;\r\n
\tb=p4ukUDSFqhqiub+zPR0DW1kp7oJZakrzupr6LBe6sUuvqpBkig56UzUwc29rFbJF\r\n
\thlX3Ov7DeYVNoN38stqwsF8ivcajXpQsXRC1cW9z8x875J041rClAjV7EGbLmudVpPX\r\n
```

```
\t4hHst1XPyX5wmgdHIhmUuh8oZKpVqGi6bHGzzf7g=\r\nFrom: sender@example.com\r\nTo:
 recipient@example.com\r\nSubject: Example subject\r\nMIME-Version: 1.0\r\nContent-
Type: text/plain; charset=UTF-8\r\nContent-Transfer-Encoding: 7bit\r\nDate: Fri, 11 Sep
 2015 20:32:32 +0000\r\nMessage-ID: <61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>
\r\nX-SES-Outgoing: 2015.09.11-54.240.9.183\r\nFeedback-ID: 1.us-east-1.Krv2FKpFdWV
+KUYw3Qd6wcpPJ4Sv/pOPpEPSHn2u2o4=:AmazonSES\r\n\r\nExample content\r\n"
}
```

Notification d'alerte

Cette section contient un exemple d'une notification Amazon SNS qui peut être déclenchée par une action S3. Les notifications déclenchées par des actions Lambda, des actions de retour à l'expéditeur, des actions d'arrêt et des actions WorkMail sont similaires. Si la notification contient des informations sur l'e-mail, elle ne contient pas le contenu de l'e-mail lui-même.

```
{
"notificationType": "Received",
"receipt": {
"timestamp": "2015-09-11T20:32:33.936Z",
"processingTimeMillis": 406,
"recipients": [
 "recipient@example.com"
],
"spamVerdict": {
 "status": "PASS"
},
"virusVerdict": {
 "status": "PASS"
},
"spfVerdict": {
 "status": "PASS"
},
"dkimVerdict": {
 "status": "PASS"
},
"action": {
 "type": "S3",
 "topicArn": "arn:aws:sns:us-east-1:012345678912:example-topic",
 "bucketName": "my-S3-bucket",
 "objectKey": "\email"
}
},
"mail": {
```

```
"timestamp": "2015-09-11T20:32:33.936Z",
"source": "0000014fbe1c09cf-7cb9f704-7531-4e53-89a1-5fa9744f5eb6-000000@amazonses.com",
"messageId": "d6iitobk75ur44p8kdnnp7g2n800",
"destination": [
 "recipient@example.com"
],
"headersTruncated": false,
"headers": [
 {
  "name": "Return-Path",
  "value":
 "<0000014fbe1c09cf-7cb9f704-7531-4e53-89a1-5fa9744f5eb6-000000@amazonses.com>"
 },
 {
  "name": "Received",
  "value": "from a9-183.smtp-out.amazonses.com (a9-183.smtp-out.amazonses.com
 [54.240.9.183]) by inbound-smtp.us-east-1.amazonaws.com with SMTP id
 d6iitobk75ur44p8kdnnp7g2n800 for recipient@example.com; Fri, 11 Sep 2015 20:32:33
 +0000 (UTC)"
 },
 {
  "name": "DKIM-Signature",
  "value": "v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple;
 s=ug7nbtf4gccmlpwj322ax3p6ow6yfsug; d=amazonses.com; t=1442003552;
 h=From:To:Subject:MIME-Version:Content-Type:Content-Transfer-Encoding:Date:Message-
ID:Feedback-ID; bh=DWr3IOmYWoXCA9ARqGC/UaODfghffiwFNRIb2Mckyt4=;
 b=p4ukUDSFqhqiub+zPR0DW1kp7oJZakrzupr6LBe6sUuvqpBkig56UzUwc29rFbJF
 hlX3Ov7DeYVNoN38stqwsF8ivcajXpQsXRC1cW9z8x875J041rClAjV7EGbLmudVpPX
 4hHst1XPyX5wmgdHIhmUuh8oZKpVqGi6bHGzzf7g="
 },
 {
  "name": "From",
  "value": "sender@example.com"
 },
 {
  "name": "To",
  "value": "recipient@example.com"
 },
 {
  "name": "Subject",
  "value": "Example subject"
 },
 {
  "name": "MIME-Version",
```

```
  "value": "1.0"
 },
 {
  "name": "Content-Type",
  "value": "text/plain; charset=UTF-8"
 },
 {
  "name": "Content-Transfer-Encoding",
  "value": "7bit"
 },
 {
  "name": "Date",
  "value": "Fri, 11 Sep 2015 20:32:32 +0000"
 },
 {
  "name": "Message-ID",
  "value": "<61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>"
 },
 {
  "name": "X-SES-Outgoing",
  "value": "2015.09.11-54.240.9.183"
 },
 {
  "name": "Feedback-ID",
  "value": "1.us-east-1.Krv2FKpFdWV+KUYw3Qd6wcpPJ4Sv/pOPpEPSHn2u2o4=:AmazonSES"
 }
],
"commonHeaders": {
 "returnPath":
 "0000014fbe1c09cf-7cb9f704-7531-4e53-89a1-5fa9744f5eb6-000000@amazonses.com",
 "from": [
  "sender@example.com"
 ],
 "date": "Fri, 11 Sep 2015 20:32:32 +0000",
 "to": [
  "recipient@example.com"
 ],
 "messageId": "<61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>",
 "subject": "Example subject"
}
}
}
```

Arrêt de l'action de jeu de règles

L'action Stop (Arrêt) met fin à l'évaluation de l'ensemble de règles de réception et vous avertit éventuellement via Amazon SNS. Cette action comporte les options suivantes.

- SNS Topic – Nom ou ARN de la rubrique Amazon SNS à avertir lorsque l'action d'arrêt est exécutée. Voici un exemple d'ARN de rubrique Amazon SNS : arn:aws:sns:us-east-1:123456789012:MyTopic. Vous pouvez également créer une rubrique Amazon SNS lorsque vous configurez une action en choisissant Create SNS Topic (Créer une rubrique SNS). Pour de plus amples informations sur les rubriques Amazon SNS, consultez le guide du développeur d'Amazon Simple Notification Service.

  > **Note**
  >
  > La rubrique Amazon SNS que vous choisissez doit être située dans la même région AWS que le point de terminaison Amazon SES que vous utilisez pour recevoir des e-mails.

Intégration à l'action Amazon WorkMail

L'action WorkMail s'intègre à Amazon WorkMail. Si Amazon WorkMail exécute l'ensemble du traitement de vos emails, vous n'utilisez généralement pas cette action directement, car Amazon WorkMail se charge de la configuration. Cette action comporte les options suivantes.

- Organization ARN – ARN de l'organisation Amazon WorkMail. Les ARN d'organisation Amazon WorkMail sont au format `arn:aws:workmail:`*`region`*`:`*`account_ID`*`:organization/`*`organization_ID`*, où :
  - `region` est la région dans laquelle vous utilisez Amazon SES et Amazon WorkMail. (Vous devez les utiliser depuis la même région.) Par exemple, us-east-1.
  - `account_ID` est l'ID de compte AWS. Vous trouverez votre ID de compte AWS sur la page Account (Compte) de la Console de gestion AWS.
  - `organization_ID` est un identifiant unique généré par Amazon WorkMail lorsque vous créez une organisation. Vous pouvez trouver l'ID d'organisation dans la console Amazon WorkMail sur la page Organization Settings (Paramètres de l'organisation) de votre organisation.

  Voici un exemple d'ARN d'organisation Amazon WorkMail complet : rn:aws:workmail:us-east-1:123456789012:organization/m-68755160c4cb4e29a2b2f8fb58f359d7. Pour plus

d'informations sur les organisations Amazon WorkMail, veuillez consulter le Guide de l'administrateur Amazon WorkMail.

- SNS Topic – Nom ou ARN de la rubrique Amazon SNS à avertir lorsque l'action Amazon WorkMail est exécutée. Voici un exemple d'ARN de rubrique Amazon SNS : arn:aws:sns:us-east-1:123456789012:MyTopic. Vous pouvez également créer une rubrique Amazon SNS lorsque vous configurez une action en choisissant Create SNS Topic (Créer une rubrique SNS). Pour de plus amples informations sur les rubriques Amazon SNS, consultez le guide du développeur d'Amazon Simple Notification Service.

  > **Note**
  >
  > La rubrique Amazon SNS que vous choisissez doit être située dans la même région AWS que le point de terminaison Amazon SES que vous utilisez pour recevoir des e-mails.

> **Note**
>
> Amazon SES prend uniquement en charge les actions WorkMail dans les régions où WorkMail est disponible. Consultez Points de terminaison et quotas Amazon WorkMail dans le Références générales AWS.

Création de filtres d'adresses IP - Démonstration de la console

Cette section vous guidera dans la configuration des filtres d'adresses IP à l'aide de la console Amazon SES. Le filtrage des adresses IP vous permet de fournir un niveau de contrôle élevé. Ces filtres IP permettent de bloquer ou d'autoriser explicitement tous les messages provenant d'adresses IP ou de plages d'adresses IP spécifiques.

Vous pouvez également utiliser l'API `CreateReceiptFilter` pour créer un filtre d'adresse IP, comme décrit dans la Référence API Amazon Simple Email Service.

> **Note**
>
> Si vous souhaitez uniquement recevoir des messages à partir d'une liste finie d'adresses IP connues, configurez une liste rouge qui contient `0.0.0.0/0` et une liste verte qui contient les adresses IP que vous approuvez. Cette configuration bloque toutes les adresses IP par

défaut, et autorise uniquement les messages provenant des adresses IP que vous spécifiez explicitement.

Conditions préalables

Les conditions préalables suivantes doivent être remplies avant de procéder à la configuration du contrôle de l'e-mail basé sur le destinataire en utilisant des filtres d'adresse IP :

1. Vous devez d'abord créer et vérifier une identité de domaine dans Amazon SES.
2. Vous devez ensuite indiquer les serveurs de messagerie qui peuvent accepter les e-mails pour votre domaine en publiant un registre MX dans les paramètres DNS de votre domaine. (Le registre MX doit faire référence au point de terminaison Amazon SES qui reçoit l'e-mail pour la région AWS où vous utilisez Amazon SES).

Création de filtres d'adresses IP

Pour créer des filtres d'adresses IP à l'aide de la console

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation de gauche, choisissez Email receiving (Réception d'e-mails).
3. Sélectionnez l'onglet IP address filters (Filtres d'adresse IP).
4. Choisissez Create Filter (Créer un filtre).
5. Saisissez un nom unique pour votre filtre. La légende du champ indique les exigences en matière de syntaxe. (Le nom doit contenir moins de 64 caractères alphanumériques, tiret (-), trait de soulignement (_) et point (.). Le nom doit commencer et se terminer par une lettre ou un chiffre).
6. Saisissez une adresse IP ou une plage d'adresses IP. La légende du champ donne des exemples spécifiques dans la syntaxe CIDR (Classless Inter-Domain Routing). (Un exemple d'une adresse IP unique est 10.0.0.1. Un exemple de plage d'adresses IP est 10.0.0.1/24. Pour en savoir plus sur la notation CIDR, voir RFC 2317).
7. Choisissez le type de stratégie en sélectionnant la case d'option Block ou Allow (Bloquer ou Autoriser).
8. Choisissez Create filter (Créer un filtre).

9. Si vous souhaitez ajouter un autre filtre IP, sélectionnez Create filter (Créer un filtre) et répétez les étapes précédentes pour chaque filtre supplémentaire que vous souhaitez ajouter.
10. Si vous souhaitez supprimer un filtre d'adresse IP, sélectionnez-le et choisissez le bouton Delete (Supprimer).

Affichage des métriques pour la réception d'e-mails via Amazon SES

Si vous avez activé la réception d'e-mails dans Amazon SES et que vous avez créé des règles de réception pour vos e-mails, vous pouvez consulter les statistiques relatives à ces ensembles de règles et règles de réception via Amazon CloudWatch.

Dans la CloudWatch console, vous trouverez les statistiques sous Mesures > Toutes les mesures > SES > Mesures définies par les règles de réception et mesures des règles de réception.

> **Note**
>
> Métriques de l'ensemble des règles de réception et Métriques de la règle de réception n'apparaîtront pas sous SES si vous n'avez pas encore :
>
> - activé la réception d'e-mails ;
> - créé de règles de réception ;
> - reçu d'e-mail correspondant à l'une de vos règles.

Les métriques de messages disponibles sont les suivantes :

- Réception de messages

Portée	Métrique	Description	Dimension
Métriques de l'ensemble des règles de réception	Received	SES a reçu un message pour lequel au moins une règle s'applique. Cette métrique peut uniquement avoir la valeur 1.	RuleSetName

Portée	Métrique	Description	Dimension
Métriques de la règle de réception	Received	SES a reçu un message et va essayer de traiter la règle appliquée. Cette métrique peut uniquement avoir la valeur 1.	RuleName

- Publication de message

Portée	Métrique	Description	Dimension
Métriques de l'ensemble des règles de réception	PublishSuccess	SES a correctement exécuté toutes les règles qui s'appliquent dans le cadre d'un ensemble de règles.	RuleSetName
Métriques de la règle de réception	PublishSuccess	SES a correctement exécuté une règle qui s'applique au message en cours de réception.	RuleName
Métriques de l'ensemble des règles de réception	PublishFailure	SES a rencontré une erreur lorsqu'il a essayé d'exécuter des règles au sein d'un ensemble de règles. L'exécution sera réessayée.	RuleSetName
Métriques de la règle de réception	PublishFailure	SES a rencontré une erreur au moment d'exécuter les actions incluses dans une règle (selon l'erreur, une nouvelle tentative d'exécution pourra avoir lieu.)	RuleName
Métriques de l'ensemble des règles de réception	PublishExpired	SES n'essaiera plus d'exécuter les règles parce qu'elles n'ont pas réussi dans les 36 heures ou parce qu'elles ont rencontré une erreur impossible à récupérer.	RuleSetName
Métriques de la règle de réception	PublishExpired	SES n'essaiera plus d'exécuter les actions de la règle car elles n'ont pas réussi dans les 36 heures.	RuleName

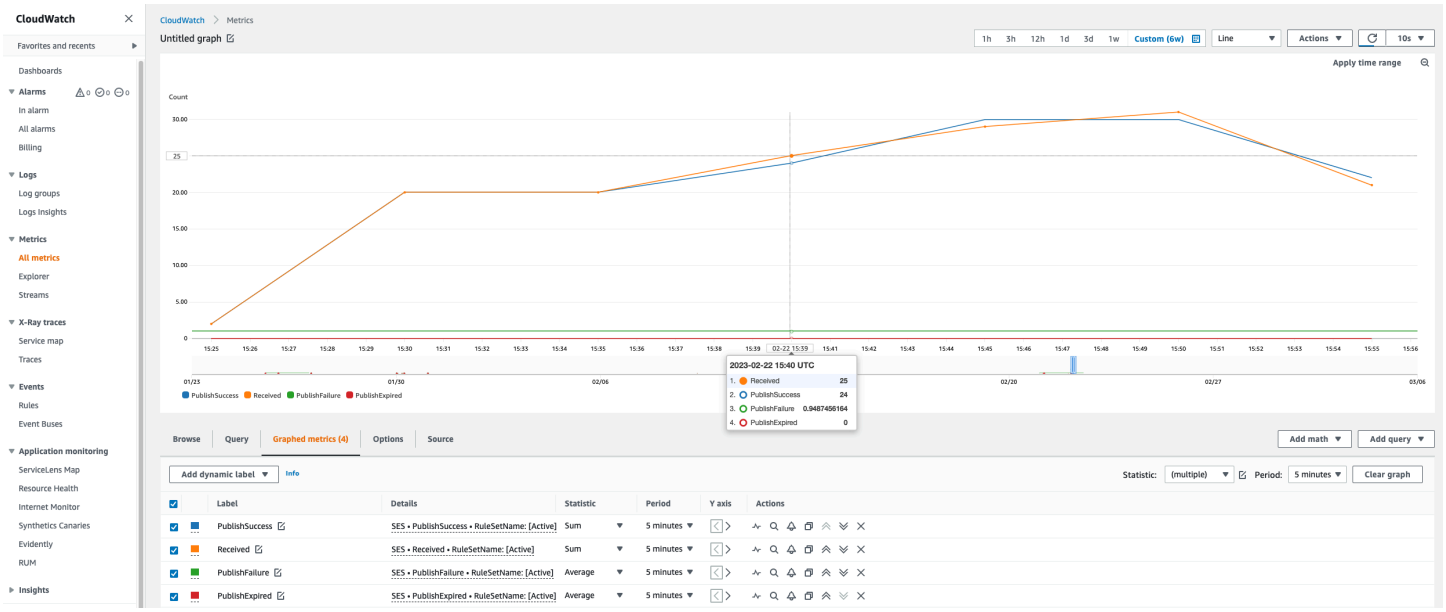
Note

- Dans les tableaux précédents, le terme « s'applique » signifie que l'expéditeur n'est pas bloqué par les filtres IP ou qu'il figure dans la liste de blocage interne de SES, et que des conditions de destinataire et la politique TLS correspondent pour la règle.
- Des erreurs liés à un échec de publication peuvent se produire si, par exemple, vous avez supprimé ou révoqué des autorisations d'accès à un compartiment Amazon S3, à une rubrique Amazon SNS ou à une fonction Lambda qu'une action incluse dans l'une de vos règles de réception devait utiliser.
- Comme un seul ensemble de règles peut être actif à la fois, SES publie un indicateur agrégé affiché sous la forme RuleSetName: [Actif] pour tous les ensembles de règles actifs pendant la période que vous avez sélectionnée CloudWatch. L'avantage est que vous pouvez modifier librement les ensembles de règles sans avoir à modifier votre configuration d'alarmes.

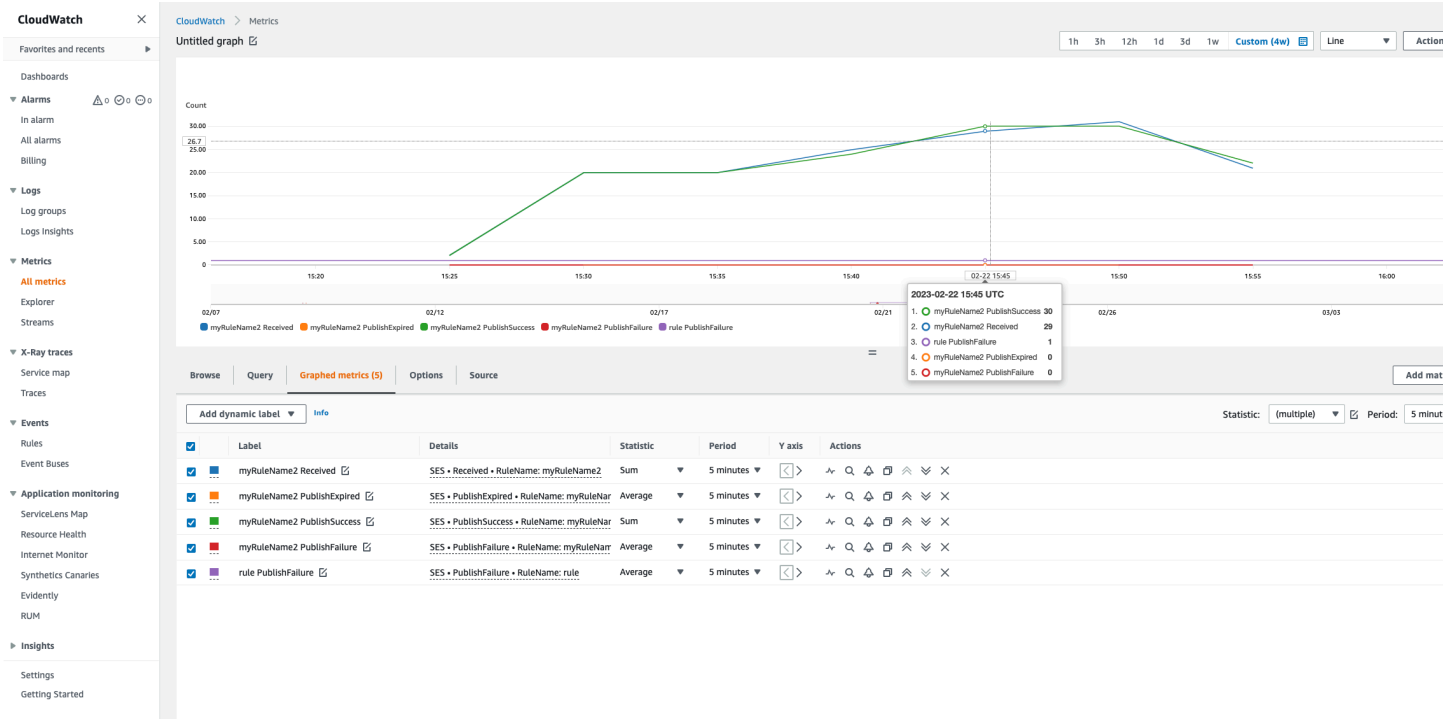
Important

Les modifications que vous apportez pour corriger votre ensemble de règles de réception s'appliquent uniquement aux e-mails qu'Amazon SES reçoit après la mise à jour. Les e-mails sont toujours évalués par rapport à l'ensemble de règles de réception qui était en vigueur au moment de leur réception.

Mesures relatives à un ensemble de règles de réception SES affichées dans la CloudWatch console.



Mesures relatives à une règle de réception SES affichées dans la CloudWatch console.



Identités vérifiées dans Amazon SES

Dans Amazon SES, une identité vérifiée est un domaine ou une adresse e-mail que vous utilisez pour envoyer ou recevoir des e-mails. Avant de pouvoir envoyer un e-mail à l'aide d'Amazon SES, vous devez vérifier chaque identité que vous utiliserez en tant qu'adresse « De », « Source », « Expéditeur » ou « Return-Path ». La vérification d'une identité auprès d'Amazon SES confirme que vous en êtes le propriétaire et évite toute utilisation non autorisée.

Si votre compte se trouve encore dans l'environnement de test (sandbox) Amazon SES, vous devez également vérifier toutes les adresses e-mails vers lesquelles vous prévoyez d'envoyer des e-mails, sauf si vous envoyez vers des boîtes de réception de test fournies par le simulateur de boîte aux lettres Amazon SES. Pour de plus amples informations, veuillez consulter the section called “Utilisation manuelle du simulateur de boîte aux lettres”.

Vous pouvez créer une identité à l'aide de la console Amazon SES ou de l'API Amazon SES. Le processus de vérification d'identité dépend du type d'identité que vous choisissez de créer.

> **Tip**
>
> Si vous utilisez SES pour la première fois, vous pouvez utiliser l'assistant Commencez pour créer et vérifier votre première identité (adresse e-mail ou domaine).

Table des matières

Vérification des identités dans Amazon SES

Dans Amazon SES, vous pouvez créer une identité au niveau du domaine ou une identité d'adresse e-mail. Ces types d'identité ne sont pas incompatibles entre eux. Dans la plupart des cas, la création d'une identité de domaine évite de devoir créer et vérifier des identités d'adresses e-mail individuelles, sauf si vous souhaitez appliquer des configurations personnalisées à une adresse e-mail spécifique. L'approche consistant à créer un domaine et à utiliser des adresses e-mail basées

sur le domaine, ou celle consistant à créer des adresses e-mail individuelles présentent toutes deux des avantages. La méthode que vous choisissez dépend de vos besoins spécifiques, comme indiqué ci-dessous.

La création et la vérification de l'identité d'une adresse e-mail est le moyen le plus rapide de démarrer avec SES, mais il y a des avantages dans le fait de vérifier une identité au niveau du domaine. Lorsque vous vérifiez l'identité d'une adresse e-mail, seule cette adresse e-mail peut être utilisée pour envoyer des e-mails, mais lorsque vous vérifiez l'identité d'un domaine, vous pouvez envoyer des e-mails à partir de n'importe quel sous-domaine ou adresse e-mail du domaine vérifié sans avoir à vérifier chacun d'entre eux individuellement. Par exemple, si vous créez et vérifiez une identité de domaine appelée exemple.com, vous n'avez pas besoin de créer des identités de sous-domaine distinctes pour a.exemple.com, a.b.exemple.com, ni des identités d'adresse e-mail distinctes pour user@example.com, user@a.example.com, etc.

Cependant, gardez à l'esprit qu'une identité d'adresse e-mail qui utilise la vérification héritée de son domaine est limitée à l'envoi d'e-mails simples. Si vous voulez effectuer des envois plus avancés, vous devrez également la vérifier explicitement en tant qu'identité d'adresse e-mail. L'envoi avancé comprend l'utilisation de l'adresse e-mail avec des jeux de configuration, des autorisations de politique pour l'envoi délégué et des configurations qui remplacent les paramètres du domaine.

Pour aider à clarifier l'héritage de vérification et les capacités d'envoi d'e-mail discutés ci-dessus, le tableau suivant catégorise chaque combinaison de vérification de domaine/adresse e-mail et liste l'héritage, le niveau d'envoi et l'état d'affichage pour chacun :

	Seulement le domaine vérifié	Seulement l'adresse e-mail vérifiée	Domaine et adresse e-mail vérifiés
Niveau d'héritage	Les sous-domaines et les adresses e-mail héritent de la vérification du domaine parent.	Adresse e-mail explicitement vérifiée.	• Les sous-domaines héritent de la vérification du domaine parent. • Adresse e-mail explicitement vérifiée.
Niveau d'envoi	Adresses e-mail limitées à l'envoi d'e-mails simples.	Adresse e-mail pouvant être utilisée dans le cadre d'un	Adresse e-mail pouvant être utilisée dans le cadre d'un

	Seulement le domaine vérifié	Seulement l'adresse e-mail vérifiée	Domaine et adresse e-mail vérifiés
		envoi d'e-mails avancés*.	envoi d'e-mails avancés*.
État affiché	État de la console/API : • Domaine/Sous-domaines = Vérifié • Adresse e-mail = Non vérifié.	État de la console/API : • Adresse e-mail = Vérifié	État de la console/API : • Domaine/Sous-domaines = Vérifié • Adresse e-mail = Vérifié.

*L'envoi avancé comprend l'utilisation de l'adresse e-mail avec des jeux de configuration, des autorisations de politique pour l'envoi délégué et des configurations qui remplacent les paramètres du domaine.

Pour envoyer des e-mails à partir du même domaine ou de la même adresse e-mail dans plus d'une région Région AWS, vous devez créer et vérifier une identité distincte pour chaque région. Vous pouvez vérifier jusqu'à 10 000 identités dans chaque région.

Lorsque vous créez et vérifiez l'identité d'une adresse e-mail, tenez compte des éléments suivants :

- Vous pouvez envoyer des e-mails à partir de n'importe quel sous-domaine ou adresse e-mail du domaine vérifié sans avoir à vérifier chacun d'entre eux individuellement. Par exemple, si vous créez et vérifiez une identité pour example.com, vous n'avez pas besoin de créer des identités distinctes pour a.example.com, a.b.example.com, user@example.com, user@a.example.com, etc.
- Comme indiqué dans la spécification RFC 1034, chaque étiquette DNS peut comporter jusqu'à 63 caractères et l'ensemble du nom de domaine ne doit pas dépasser une longueur totale de 255 caractères.
- Si vous vérifiez un domaine, un sous-domaine ou une adresse e-mail qui partage un domaine racine, les paramètres d'identité (tels que les notifications de retour) s'appliquent au niveau le plus détaillé que vous avez vérifié.
  - Les paramètres d'identité de l'adresse électronique vérifiée remplacent les paramètres d'identité du domaine vérifié.

- Les paramètres d'identité de sous-domaine vérifiés ont priorité sur les paramètres d'identité de domaine vérifiés, les paramètres de sous-domaine de niveau inférieur étant prioritaires sur les paramètres de sous-domaine de niveau supérieur.

  Par exemple, supposons que vous vérifiez utilisateur@a.b.exemple.com, a.b.exemple.com, b.exemple.com et exemple.com. Voici les paramètres d'identité vérifiée qui seront utilisés dans les scénarios suivants :

  - Les e-mails envoyés depuis utilisateur@exemple.com (une adresse qui n'est pas vérifiée spécifiquement) utilisent les paramètres pour exemple.com.
  - Les e-mails envoyés depuis utilisateur@a.b.example.com (une adresse e-mail qui est vérifiée spécifiquement) utilisent les paramètres pour utilisateur@a.b.example.com.
  - Les e-mails envoyés depuis utilisateur@b.exemple.com (une adresse e-mail qui n'est pas vérifiée spécifiquement) utilisent les paramètres pour b.exemple.com.

- Vous pouvez ajouter des étiquettes aux adresses e-mail vérifiées sans effectuer d'autres étapes de vérification. Pour ajouter une étiquette à une adresse e-mail, ajoutez un signe plus (+) entre le nom de compte et l'arobase (@), suivis d'une étiquette de texte. Par exemple, si vous avez déjà vérifié expediteur@exemple.com, vous pouvez utiliser expediteur+monEtiquette@exemple.com comme adresse « De » ou « Return-Path (Chemin de retour) » pour vos e-mails. Vous pouvez utiliser cette fonction pour implémenter la méthode de l'adresse de retour variable (VERP). Vous pouvez ensuite utiliser VERP pour détecter et supprimer de vos listes de diffusion les adresses e-mail à partir desquelles les messages ne peuvent pas être remis.
- Les noms de domaine ne sont pas sensibles à la casse. Si vous vérifiez exemple.com, vous pouvez envoyer des messages depuis EXEMPLE.com également.
- Les adresses e-mail sont sensibles à la casse. Si vous vérifiez expediteur@EXEMPLE.com, vous ne pouvez pas envoyer d'e-mail depuis expediteur@exemple.com, sauf si vous vérifiez également expediteur@exemple.com.
- Dans chaque Région AWS, vous pouvez vérifier jusqu'à 10 000 identités (domaines et adresses e-mail, dans n'importe quelle combinaison).

> **Tip**
>
> Si vous utilisez SES pour la première fois, vous pouvez utiliser l'assistant Commencez pour créer et vérifier votre première identité (adresse e-mail ou domaine).

Table des matières

Création d'une identité de domaine

Une partie de la création d'une identité de domaine consiste à configurer sa vérification basée sur DKIM. Le standard DKIM (DomainKeys Identified Mail) est une méthode d'authentification des e-mails que Amazon SES utilise pour vérifier la propriété du domaine, et que les serveurs de messagerie destinataires utilisent pour valider l'authenticité des e-mails. Vous pouvez choisir de configurer DKIM en utilisant soit Easy DKIM soit Bring Your Own DKIM (BYODKIM). Selon la méthode choisie, vous devrez configurer la longueur de la clé de signature de la clé privée comme suit :

- Easy DKIM – Vous pouvez soit accepter la valeur par défaut de 2048 bits d'Amazon SES, soit la remplacer en sélectionnant 1024 bits.
- BYODKIM - La longueur de la clé privée doit être comprise entre 1024 bits au minimum et 2048 bits au maximum.

Voir the section called “Longueur de la clé DKIM” pour en savoir plus sur les longueurs des clés de signature DKIM et sur la manière de les modifier.

La procédure suivante vous montre comment créer une identité de domaine à l'aide de la console Amazon SES.

- Si vous avez déjà créé votre domaine et que vous devez simplement le vérifier, passez à la procédure the section called “Vérification d'une identité de domaine” sur cette page.

Pour créer une identité de domaine

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES sur la page https://console.aws.amazon.com/ses/.

2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).
3. Choisissez Create identity (Créer une identité).
4. Sous Identity details (Détails relatifs à l'identité), sélectionnez Domain (Domaine) en tant que type d'identité que vous souhaitez créer. Vous devez avoir accès aux paramètres DNS du domaine pour finaliser le processus de vérification du domaine.
5. Entrez le nom de domaine ou de sous-domaine dans le champ Domain (Domaine).

   > **Tip**
   >
   > Si votre domaine est www.example.com, saisissez example.com comme domaine. N'incluez pas le « www. » Si vous le faites, le processus de vérification du domaine ne réussira pas.

6. (Facultatif) Si vous souhaitez attribuer un jeu de configuration par défaut, cochez la case.

   1. Pour jeu de configuration par défaut, sélectionnez le jeu de configurations existant que vous souhaitez attribuer à votre identité. Si vous n'avez pas encore créé de jeux de configuration, consultez Jeux de configurations.

      > **Note**
      >
      > Amazon SES utilise par défaut le jeu de configuration affecté uniquement lorsqu'aucun autre ensemble n'est spécifié au moment de l'envoi. Si un jeu de configuration est spécifié, Amazon SES applique l'ensemble spécifié à la place de l'ensemble par défaut.

7. (Facultatif) Si vous souhaitez utiliser un domaine MAIL FROM personnalisé, cochez la case et effectuez les étapes suivantes. Pour plus d'informations, consultez the section called “Utilisation d'un domaine MAIL FROM personnalisé”.

   1. Pour MAIL FROM domain (Domaine MAIL FROM), entrez le sous-domaine que vous souhaitez utiliser en tant que domaine MAIL FROM. Ce doit être un sous-domaine de l'identité de domaine que vous vérifiez. Le domaine MAIL FROM ne doit pas être un domaine à partir duquel vous envoyez des e-mails.

2. Pour Behavior on MX failure (Comportement en cas d'échec MX), indiquez l'action qu'Amazon SES doit prendre s'il ne trouve pas le registre MX requis au moment de l'envoi. Choisissez l'une des options suivantes :
   - Utiliser le domaine MAIL FROM par défaut – Si le registre MX du domaine MAIL FROM n'est pas configuré correctement, Amazon SES utilise un sous-domaine d'amazonses.com. Le sous-domaine varie en fonction de la Région AWS dans laquelle vous utilisez Amazon SES.
   - Rejeter le message : si le registre MX du domaine MAIL FROM personnalisé n'est pas configuré correctement, Amazon SES renvoie une erreur `MailFromDomainNotVerified`. Si vous choisissez cette option, les e-mails que vous essayez d'envoyer à partir de ce domaine sont automatiquement rejetés.
3. Pour Publish DNS records to Route53 (Publier des enregistrements DNS sur Route53), si votre domaine est hébergé via Amazon Route 53, vous avez la possibilité de laisser SES publier les enregistrements TXT et MX associés au moment de la création en laissant la case Enabled (Activé) cochée. Si vous préférez publier ces enregistrements ultérieurement, décochez la case Enabled (Activé). (Vous pouvez revenir ultérieurement pour publier les enregistrements sur Route 53 en modifiant l'identité – veuillez consulter la section the section called “Modification d'une identité à l'aide de la console”.)

8. (Facultatif) Pour configurer la vérification personnalisée basée sur DKIM en dehors du paramètre SES par défaut qui utilise Easy DKIM avec une longueur de chant de 2048 bits, sous Verifying your domain (Vérification de votre domaine), développez Advanced DKIM settings (Paramètres avancés DKIM) et choisissez le type de DKIM que vous souhaitez configurer :

   a. Easy DKIM :

      i. Dans le champ Identity type (Type d'identité), choisissez Easy DKIM.

      ii. Dans DKIM signing key length (Longueur de clé de signature DKIM), choisissez RSA_2048_BIT ou RSA_1024_BIT.

      iii. Pour Publish DNS records to Route53 (Publier des enregistrements DNS sur Route53), si votre domaine est hébergé via Amazon Route 53, vous avez la possibilité de laisser SES publier les enregistrements CNAME associés au moment de la création en laissant la case Enabled (Activé) cochée. Si vous préférez publier ces enregistrements ultérieurement, décochez la case Enabled (Activé). (Vous pouvez revenir ultérieurement pour publier les enregistrements sur Route 53 en modifiant l'identité – veuillez consulter la section the section called “Modification d'une identité à l'aide de la console”.)

   b. (Fournir un jeton d'authentification DKIM (BYODKIM) :

i. Assurez-vous que vous avez déjà généré une paire de clés publique-privée et que vous avez ajouté la clé publique à votre fournisseur d'hôtes DNS. Pour de plus amples informations, veuillez consulter the section called “BYODKIM - Bring Your Own DKIM (Fournissez votre propre DKIM)”.

ii. Dans le champ Identity type (Type d'identité), choisissez Provide DKIM authentication token (BYODKIM) (Fournir un jeton d'authentification DKIM (BYODKIM)).

iii. Pour Private key (Clé privée), collez la clé privée que vous avez générée à partir de votre paire de clés publique-privée. La clé privée doit utiliser le chiffrement RSA d'au moins 1024 bits et jusqu'à 2048 bits, et doit être chiffré en utilisant le chiffrement (PEM) base64.

> **Note**
>
> Vous devez supprimer les première et dernière lignes (respectivement `-----BEGIN PRIVATE KEY-----` et `-----END PRIVATE KEY-----`) de la clé privée générée. En outre, vous devez supprimer les sauts de ligne dans la clé privée générée. La valeur résultante est une chaîne de caractères sans espace ni saut de ligne.

iv. Pour Selector name (Nom du sélecteur), saisissez le nom du sélecteur à spécifier dans les paramètres DNS de votre domaine.

9. Dans DKIM signatures (Signatures DKIM), assurez-vous que la case Enabled (Activé) est bien coché.
10. (Facultatif) Ajoutez une ou plusieurs balises à votre identité de domaine en incluant une clé de balise et une valeur facultative pour la clé :
    1. Choisissez Add new tag (Ajouter une nouvelle balise) et entrez la Clé. Vous pouvez aussi ajouter une valeur pour la balise.
    2. Répétez la procédure pour que les balises supplémentaires ne dépassent pas 50, ou choisissez Remove (Supprimer) pour supprimer des balises.
11. Choisissez Create identity (Créer une identité).

Maintenant que vous avez configuré votre identité de domaine avec DKIM, vous devez terminer le processus de vérification avec votre fournisseur DNS. Passez à the section called “Vérification d'une

identité de domaine” et suivez les procédures d'authentification DNS pour le type de DKIM avec lequel vous avez configuré votre identité.

Vérification d’une identité de domaine DKIM auprès de votre fournisseur DNS

Une fois que vous avez créé votre identité de domaine configurée avec DKIM, vous devez terminer le processus de vérification avec votre fournisseur DNS en suivant les procédures d'authentification respectives pour le type de DKIM que vous avez choisi.

Si vous n'avez pas créé d'identité de domaine, consultez the section called “Création d'une identité de domaine”.

> **Note**
>
> La vérification d'une identité de domaine nécessite l'accès aux paramètres DNS du domaine. La propagation de ces paramètres peut prendre jusqu'à 72 heures.

Pour vérifier un domaine DKIM auprès de votre fournisseur DNS

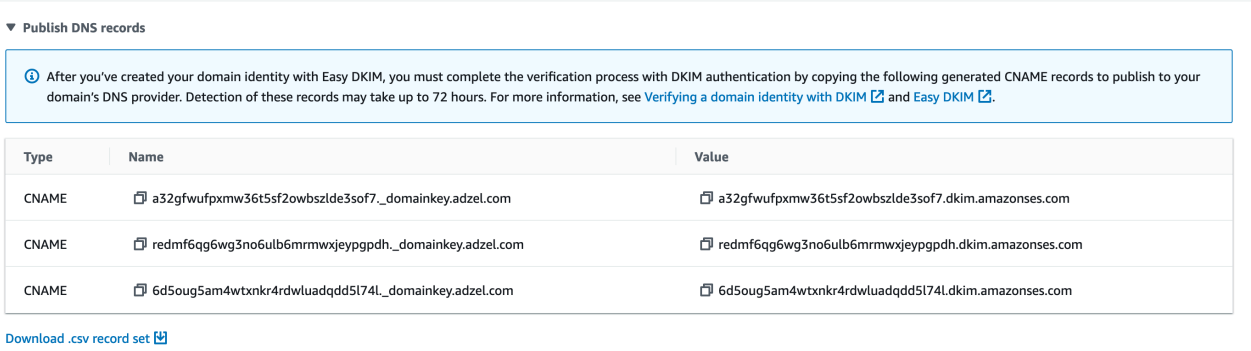
1. Depuis la table Loaded identities (Identités chargées), sélectionnez le domaine que vous souhaitez vérifier.
2. Dans l'onglet Authentification de la page de détails de l'identité, développez Publish DNS records (Publier les registres DNS).
3. Selon la version de DKIM avec laquelle vous avez configuré votre domaine, Easy DKIM ou BYODKIM, suivez les instructions respectives :

   Easy DKIM

   Pour vérifier un domaine configuré avec Easy DKIM

   1. Depuis la table Publish DNS records (Publier les registres DNS), copiez les trois registres CNAME apparaissant dans cette section qui doivent être publiés (ajoutés) sur votre fournisseur DNS. Sinon, vous pouvez choisir Download Record Set as CSV (Télécharger le jeu de registres au format .csv) pour enregistrer une copie des registres sur votre ordinateur.

L'image suivante présente un exemple de registres CNAME à publier sur votre fournisseur DNS.



2. Ajoutez les registres CNAME aux paramètres DNS de votre domaine, indépendamment de votre fournisseur d'hôte DNS :

   - Tous les fournisseurs d'hôte DNS (sauf Route 53) : connectez-vous au DNS ou au fournisseur d'hébergement web de votre domaine, puis ajoutez les registres CNAME comportant les valeurs que vous avez copiées ou enregistrées. Les différents fournisseurs ont des procédures différentes pour mettre à jour les registres DNS. Veuillez consulter la table de fournisseur d'hôte DNS en suivant ces procédures.

     > **Note**
     >
     > Un petit nombre de fournisseurs DNS n'autorisent pas l'inclusion de traits de soulignement (_) dans les noms de registre. Cependant, les traits de soulignement dans les noms de registres DKIM sont obligatoires. Si votre fournisseur DNS ne vous permet pas de saisir un caractère de soulignement dans le nom de registre, contactez l'équipe de support client du fournisseur pour obtenir de l'aide.

   - Route 53 comme fournisseur d'hôte DNS : si vous utilisez Route 53 sur le même compte que celui que vous utilisez pour envoyer des e-mails avec SES, et que le domaine est enregistré, SES met automatiquement à jour les paramètres DNS pour votre domaine si vous avez autorisé SES à les publier au moment de la création. Sinon, vous pouvez facilement les publier sur Route 53 en cliquant sur un bouton après leur création : veuillez consulter the section called “Modification d'une identité à l'aide de la console”. Si vos paramètres DNS ne se mettent pas à jour automatiquement, ou si vous souhaitez ajouter à Route 53 des enregistrements

CNAME qui ne se trouvent pas sur le même compte que celui que vous utilisez pour envoyer des e-mails via SES, suivez les procédures décrites dans Modification des enregistrements.

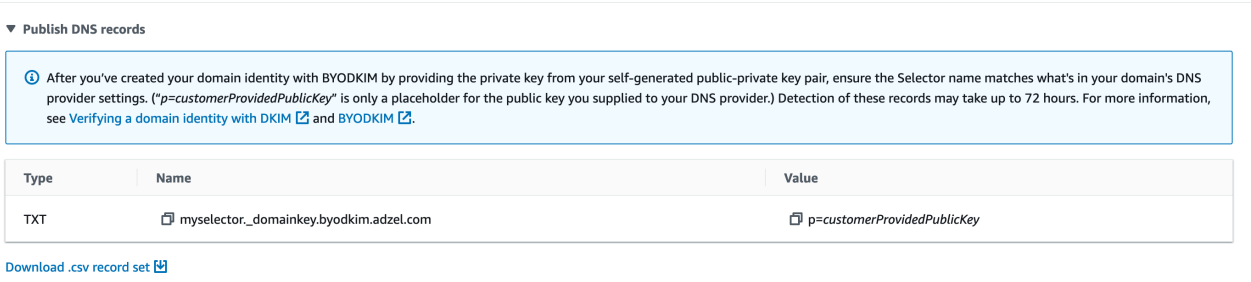
- Si vous n'êtes pas sûr de savoir qui est votre fournisseur DNS – Renseignez-vous auprès de votre administrateur système.

BYODKIM

Pour vérifier un domaine configuré avec BYODKIM

1. Pour résumer, lorsque vous avez créé votre domaine ou configuré un domaine existant avec BYODKIM, vous avez ajouté la clé privée (à partir de votre paire de clés publique-privée auto-générée) et le préfixe du nom du sélecteur dans leurs champs respectifs sur la page Advanced DKIM Settings (Paramètres avancés DKIM) de la console SES. Vous devez maintenant terminer le processus de vérification en mettant à jour les registres suivants pour votre fournisseur d'hôte DNS.
2. Depuis la table Publish DNS records (Publier les registres DNS), copiez le registre du nom du sélecteur apparaissant dans la colonne Name (Nom) qui doit être publié (ajouté) sur votre fournisseur DNS. Sinon, vous pouvez choisir Download .csv record set (Télécharger le jeu de registres .csv) pour en enregistrer une copie sur votre ordinateur.

   L'image suivante présente un exemple de registre de nom de sélecteur à publier sur votre fournisseur DNS.



3. Connectez-vous au fournisseur DNS ou d'hébergement web de votre domaine, puis ajoutez le registre de nom de sélecteur que vous avez copié ou enregistré. Les différents fournisseurs ont des procédures différentes pour mettre à jour les registres DNS. Veuillez consulter la table de fournisseur d'hôte DNS en suivant ces procédures.

> **Note**
>
> Un petit nombre de fournisseurs DNS n'autorisent pas l'inclusion de traits de soulignement (_) dans les noms de registre. Cependant, les traits de soulignement dans les noms de registres DKIM sont obligatoires. Si votre fournisseur DNS ne vous permet pas de saisir un caractère de soulignement dans le nom de registre, contactez l'équipe de support client du fournisseur pour obtenir de l'aide.

4. Si ce n'est pas déjà fait, assurez-vous d'ajouter la clé publique de votre paire de clés publique-privée auto-générée au fournisseur DNS ou d'hébergement web de votre domaine.

   Notez que dans la table Publish DNS records (Publier les registres DNS), le registre de clé publique qui apparaît dans la colonne Value (Valeur) affiche uniquement, « p=customerProvidedPublicKey », comme espace réservé pour la clé publique que vous avez enregistrée sur votre ordinateur ou fournie à votre fournisseur DNS.

   > **Note**
   >
   > Lorsque vous publiez (ajoutez) votre clé publique à votre fournisseur DNS, elle doit être formatée comme suit :
   >
   > - Vous devez supprimer les première et dernière lignes (respectivement `-----BEGIN PUBLIC KEY-----` et `-----END PUBLIC KEY-----`) de la clé publique générée. En outre, vous devez supprimer les sauts de ligne dans la clé publique générée. La valeur résultante est une chaîne de caractères sans espace ni saut de ligne.
   > - Vous devez inclure le préfixe p= comme indiqué dans la colonne Value (Valeur) de la table Publish DNS records (Publier des enregistrements DNS).

4. La propagation des modifications des paramètres DNS peut prendre jusqu'à 72 heures. Dès qu'Amazon SES détecte tous les registres DKIM requis dans les paramètres DNS de votre domaine, le processus de vérification est terminé. La configuration de DKIM de votre domaine apparaît comme Successful (Réussie) et le Statut d'identité (Identity status) apparaît comme Verified (Vérifié).

5. Si vous souhaitez configurer et vérifier un domaine MAIL FROM personnalisé, suivez les procédures décrites dans Configuration de votre domaine MAIL FROM personnalisé.

Le tableau suivant comprend des liens vers de la documentation relative quelques fournisseurs DNS courants. Cette liste n'est pas exhaustive et n'a pas valeur d'approbation. De même, si votre fournisseur DNS n'est pas répertorié, cela ne signifie pas que vous ne pouvez pas utiliser le domaine avec Amazon SES.

Fournisseur DNS/d'hébergement	Lien vers la documentation
GoDaddy	Ajouter un enregistrement CNAME (lien externe)
DreamHost	How do I add custom DNS records? (Comment ajouter des registres DNS personnalisés ?) (lien externe)
Cloudflare	Gestion des registres DNS dans CloudFlare (lien externe)
HostGator	Manage DNS Records with HostGator/eNom (Gérer des registres DNS avec HostGator/eNom) (lien externe)
Namecheap	How do I add TXT/SPF/DKIM/DMARC records for my domain? (Comment ajouter des registres TXT/SPF/DKIM/DMARC pour mon domaine ?) (lien externe)
Names.co.uk	Changing your domains DNS Settings (Modifier vos paramètres DNS de domaine) (lien externe)
Wix	Ajouter ou mettre à jour des enregistrements CNAME sur votre compte Wix (lien externe)

Résolution des problèmes de vérification de domaine

Si vous avez appliqué les étapes ci-dessus mais que votre domaine n'est pas vérifié au bout de 72 heures, vérifiez les points suivants :

- Vérifiez que vous avez saisi les valeurs de vos registres DNS dans les champs appropriés. Certains fournisseurs DNS font référence au champ Name/host (Nom/hôte) en tant qu'hôte ou nom d'hôte. De plus, certains fournisseurs font référence au champ Record value (Valeur de registre) en tant que champ Points to (Pointe vers) ou Result (Résultat).
- Assurez-vous que votre fournisseur n'a pas ajouté automatiquement votre nom de domaine à la fin de la valeur Name/host (Nom/hôte) que vous avez entrée dans le registre DNS. Certains fournisseurs ajoutent le nom de domaine sans indiquer qu'ils le font. Si votre fournisseur a ajouté votre nom de domaine à la fin de la valeur Name/host (Nom/hôte), supprimez le nom de domaine à la fin de la valeur. Vous pouvez également essayer d'ajouter un point à la fin de la valeur dans le registre DNS. Ce point indique au fournisseur que le nom de domaine est complet.
- Le trait de soulignement (_) est obligatoire dans la valeur Name/host (Nom/hôte) de chaque registre DNS. Si votre fournisseur n'autorise pas les traits de soulignement dans les noms des registres DNS, contactez le service de support client du fournisseur pour obtenir une aide supplémentaire.
- Les registres de validation que vous devez ajouter à la configuration DNS de votre domaine sont différents pour chaque Région AWS. Si vous voulez utiliser un domaine pour envoyer des e-mails depuis plusieurs Régions AWS, vous devez vérifier le domaine dans chacune de ces régions.

Création d'une identité d'adresse e-mail

Effectuez la procédure suivante pour créer l'identité d'une adresse e-mail en utilisant la console Amazon SES.

Pour créer une identité d'adresse e-mail (console)

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).
3. Choisissez Create identity (Créer une identité).

4. Sous Identity details (Détails relatifs à l'identité), sélectionnez Domain (Domaine) en tant que type d'identité que vous souhaitez créer.
5. Pour Email address (Adresse e-mail), saisissez l'adresse e-mail à utiliser. L'adresse e-mail doit être une adresse pouvant recevoir du courrier et à laquelle vous avez accès.
6. (Facultatif) Si vous souhaitez attribuer un jeu de configuration par défaut, cochez la case.

    1. Pour jeu de configuration par défaut, sélectionnez le jeu de configurations existant que vous souhaitez attribuer à votre identité. Si vous n'avez pas encore créé de jeux de configuration, consultez Jeux de configurations.

    > **Note**
    >
    > Amazon SES utilise par défaut le jeu de configuration affecté uniquement lorsqu'aucun autre ensemble n'est spécifié au moment de l'envoi. Si un jeu de configuration est spécifié, Amazon SES applique l'ensemble spécifié à la place de l'ensemble par défaut.

7. (Facultatif) Ajoutez une ou plusieurs balises à votre identité de domaine en incluant une clé de balise et une valeur facultative pour la clé :

    1. Choisissez Add new tag (Ajouter une nouvelle balise) et entrez la Clé. Vous pouvez aussi ajouter une valeur pour la balise.
    2. Répétez la procédure pour que les balises supplémentaires ne dépassent pas 50, ou choisissez Remove (Supprimer) pour supprimer des balises.

8. Pour créer votre identité d'adresse e-mail, choisissez Create identity (Créer une identité). Une fois qu'il a été créé, vous devez recevoir un e-mail de vérification dans les cinq minutes. L'étape suivante consiste à vérifier votre adresse e-mail en suivant la procédure de vérification dans la section suivante.

> **Note**
>
> Vous pouvez personnaliser les messages qui sont envoyés aux adresses e-mail que vous essayez de vérifier. Pour de plus amples informations, veuillez consulter the section called “Utilisation de modèles d'e-mail de vérification personnalisé”.

Maintenant que vous avez créé l'identité de votre adresse e-mail, vous devez terminer le processus de vérification. Passez à the section called “Vérification d'une identité d'adresse e-mail”.

Vérification d'une identité d'adresse e-mail

Une fois que vous avez créé l'identité de votre adresse e-mail, vous devez terminer le processus de vérification.

Si vous n'avez pas créé d'identité d'adresse e-mail, consultez the section called “Création d'une identité d'adresse e-mail”.

Pour vérifier l'identité d'une adresse e-mail

1. Vérifiez la boîte de réception de l'adresse e-mail utilisée pour créer votre identité et recherchez un e-mail de no-reply-aws@amazon.com.
2. Ouvrez cet e-mail et cliquez sur le lien qui y est fourni pour terminer le processus de vérification de l'adresse e-mail. Une fois qu'il est terminé, le Identity status (Statut d'identité) passe à Verified (Vérifié).

Résoudre les problèmes de vérification d'adresses e-mail

Si vous ne recevez pas l'e-mail de vérification dans les cinq minutes suivant la création de votre identité, essayez les étapes suivantes pour résoudre le problème :

- Vérifiez que l'adresse saisie est correcte.
- Vérifiez que l'adresse e-mail que vous tentez de vérifier peut recevoir des e-mails. Vous pouvez tester cela en utilisant une autre adresse e-mail pour envoyer un e-mail de test à l'adresse à vérifier.
- Vérifiez dans le dossier du courrier indésirable.
- Le lien fourni dans l'e-mail de vérification expire après 24 heures. Pour envoyer un nouvel e-mail de vérification, choisissez Renvoi en haut de la page des détails d'identité.

Créez et vérifiez une identité et attribuez un jeu de configuration par défaut en même temps

Vous pouvez utiliser l'opération CreateEmailIdentity dans l'API Amazon SES v2 pour créer une nouvelle identité d'adresse e-mail et définir en même temps sa configuration par défaut définie.

> **Note**
>
> Avant d'effectuer la procédure complète décrite dans cette section, vous devez installer et configurer l' AWS CLI. Pour en savoir plus, veuillez consulter le Guide de l'utilisateur AWS Command Line Interface.

Pour définir un ensemble de configurations par défaut à l'aide de la AWS CLI

- Sur la ligne de commande, saisissez la commande suivante pour créer un modèle à l'aide de l'opération CreateEmailIdentity.

```
aws sesv2 create-email-identity --email-identity ADDRESS-OR-DOMAIN --configuration-set-name CONFIG-SET
```

Dans les commandes précédentes, remplacez *ADDRESS-OR-DOMAIN* par l'identité d'adresse e-mail que vous souhaitez vérifier. Remplacez *CONFIG-SET* par le nom du jeu de configurations que vous souhaitez définir comme jeu de configurations par défaut pour l'identité.

Si la commande s'exécute correctement, elle se termine sans fournir de sortie.

Pour vérifier votre adresse e-mail

1. Contrôlez la boîte de réception pour l'adresse e-mail que vous êtes en train de vérifier. Vous recevrez un message avec la ligne d'objet suivante : « Amazon Web Services – Demande de vérification d'adresse e-mail dans la région *Nomderégion* », où *Nomderégion* est le nom de la Région AWS dans laquelle vous avez tenté de vérifier l'adresse e-mail.

   Ouvrez le message, puis cliquez sur le lien qui s'y trouve.

   > **Note**
   >
   > Le lien du message de vérification expire 24 heures après l'envoi du message. Si 24 heures se sont écoulées depuis que vous avez reçu l'e-mail de vérification, répétez les étapes 1 à 5 pour recevoir un e-mail de vérification contenant un lien valide.

2. Dans la console Amazon SES, sous Identity Management (Gestion des identités), choisissez Email Addresses (Adresses e-mail). Dans la liste des adresses e-mail, recherchez l'adresse e-

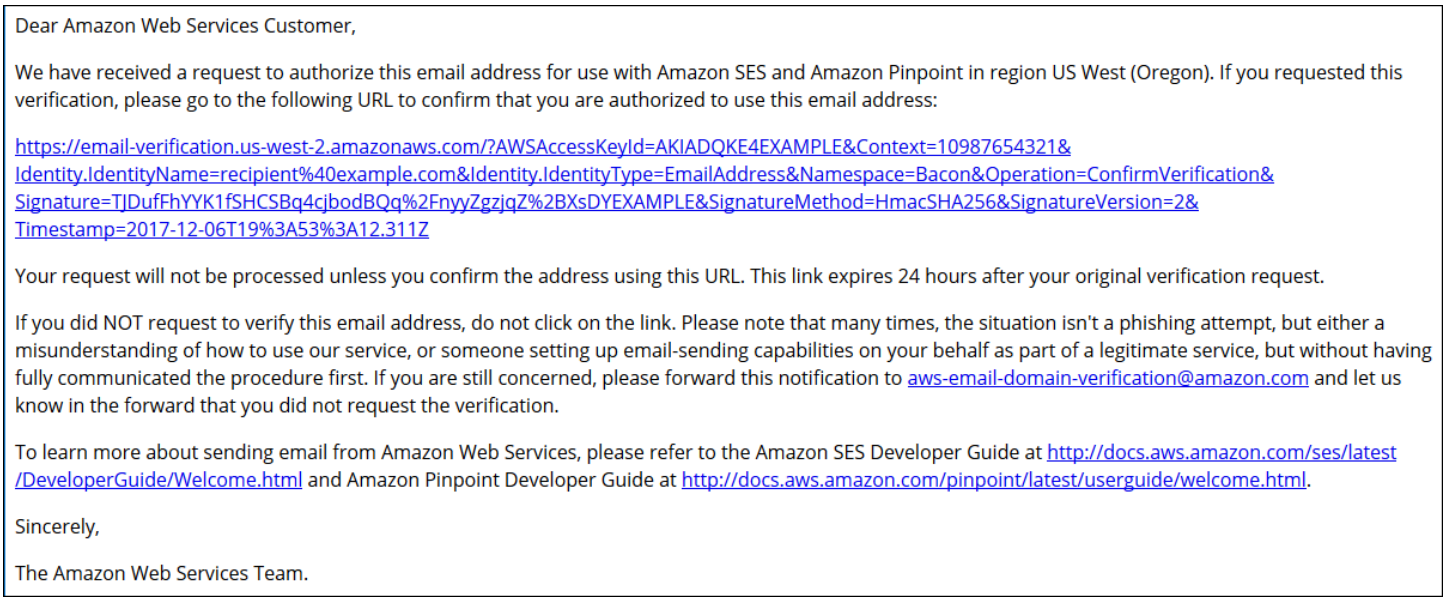
mail que vous vérifiez. Si l'adresse e-mail a été vérifiée, la valeur dans la colonne Status indique « verified ».

Pour vérifier votre domaine

Si vous avez saisi un nom de domaine pour le paramètre `--email-identity` dans la procédure de ligne de commande ci-dessus, consultez Vérification d'une identité de domaine pour en savoir plus.

Utilisation de modèles d'e-mail de vérification personnalisé

Lorsque vous essayez de vérifier une adresse e-mail, Amazon SES envoie à cette adresse un e-mail semblable à l'exemple présenté dans l'image suivante.



Dear Amazon Web Services Customer,

We have received a request to authorize this email address for use with Amazon SES and Amazon Pinpoint in region US West (Oregon). If you requested this verification, please go to the following URL to confirm that you are authorized to use this email address:

https://email-verification.us-west-2.amazonaws.com/?AWSAccessKeyId=AKIADQKE4EXAMPLE&Context=10987654321&Identity.IdentityName=recipient%40example.com&Identity.IdentityType=EmailAddress&Namespace=Bacon&Operation=ConfirmVerification&Signature=TJDufFhYYK1fSHCSBq4cjbodBQq%2FnyyZgzjqZ%2BXsDYEXAMPLE&SignatureMethod=HmacSHA256&SignatureVersion=2&Timestamp=2017-12-06T19%3A53%3A12.311Z

Your request will not be processed unless you confirm the address using this URL. This link expires 24 hours after your original verification request.

If you did NOT request to verify this email address, do not click on the link. Please note that many times, the situation isn't a phishing attempt, but either a misunderstanding of how to use our service, or someone setting up email-sending capabilities on your behalf as part of a legitimate service, but without having fully communicated the procedure first. If you are still concerned, please forward this notification to aws-email-domain-verification@amazon.com and let us know in the forward that you did not request the verification.

To learn more about sending email from Amazon Web Services, please refer to the Amazon SES Developer Guide at http://docs.aws.amazon.com/ses/latest/DeveloperGuide/Welcome.html and Amazon Pinpoint Developer Guide at http://docs.aws.amazon.com/pinpoint/latest/userguide/welcome.html.

Sincerely,

The Amazon Web Services Team.

Plusieurs clients Amazon SES créent des applications (par exemple, des suites d'applications de marketing électronique ou des systèmes de tickets) qui envoient des e-mails via Amazon SES au nom de leurs propres clients. Pour les utilisateurs finaux de ces applications, le processus de vérification par e-mail peut être déroutant : l'e-mail de vérification utilise des éléments Amazon SES personnalisés plutôt que ceux de l'application, alors que ces utilisateurs finaux ne se sont jamais inscrits pour utiliser Amazon SES directement.

Si votre cas d'utilisation Amazon SES nécessite que vos clients aient besoin que leurs adresses e-mail soient vérifiées pour être utilisées avec Amazon SES, vous pouvez créer des e-mails de vérification personnalisés. Ces e-mails personnalisés vous aident à réduire la confusion du client et à augmenter la vitesse à laquelle vos clients finalisent le processus d'inscription.

> **Note**
>
> Pour utiliser cette fonction, votre compte Amazon SES doit se trouver hors de l'environnement de test (sandbox). Pour plus d'informations, consultez Demande d'accès à la production (sortie du sandbox d'Amazon SES).

Rubriques de cette section :

- Création d'un modèle d'e-mail de vérification personnalisé
- Modification d'un modèle d'e-mail de vérification personnalisé
- Envoi d'e-mails de vérification à l'aide de modèles personnalisés
- Questions fréquentes sur l'e-mail de vérification personnalisé

Création d'un modèle d'e-mail de vérification personnalisé

Pour créer un e-mail de vérification personnalisé, utilisez l'opération d'API `CreateCustomVerificationEmailTemplate`. Cette opération utilise les entrées suivantes :

Attribut	Description
`TemplateName`	Nom du modèle. Le nom que vous spécifiez doit être unique.
`FromEmailAddress`	Adresse e-mail à partir de laquelle l'e-mail de vérification est envoyé. L'adresse ou le domaine que vous spécifiez doit être vérifié pour une utilisation avec votre compte Amazon SES. **Note** L'attribut `FromEmailAddress` ne prend pas en charge les noms d'affichage (également appelés « noms d'expéditeur convivial »).
`TemplateSubject`	Ligne d'objet de l'e-mail de vérification.

Attribut	Description
`TemplateContent`	Corps de l'e-mail. Le corps de l'e-mail peut contenir du code HTML, avec certaines restrictions. Pour plus d'informations, consultez Questions fréquentes sur l'e-mail de vérification personnalisé.
`SuccessRedirectionURL`	URL vers laquelle les utilisateurs sont renvoyés si leurs adresses e-mail sont validées.
`FailureRedirectionURL`	URL vers laquelle les utilisateurs sont renvoyés si leurs adresses e-mail ne sont pas validées.

Vous pouvez utiliser les kits SDK AWS ou l'AWS CLI pour créer un modèle d'e-mail de vérification personnalisé avec l'opération `CreateCustomVerificationEmailTemplate`. Pour en savoir plus sur les kits SDK AWS, consultez Outils pour Amazon Web Services. Pour en savoir plus sur l'AWS CLI, consultez Interface de ligne de commande AWS.

La section suivante inclut des procédures pour la création d'un e-mail de vérification personnalisé à l'aide de l' AWS CLI. Ces procédures supposent que vous avez installé et configuré l' AWS CLI. Pour en savoir plus sur l'installation et la configuration de l'AWS CLI, consultez le Guide de l'utilisateur de l'AWS Command Line Interface.

> **Note**
>
> Pour effectuer la procédure décrite dans cette section, vous devez utiliser la version 1.14.6 ou ultérieure de l' AWS CLI. Pour de meilleurs résultats, passez à la dernière version de l' AWS CLI. Pour plus d'informations sur l'installation ou la mise à jour de l'AWS CLI, veuillez consulter la page relative à l'installation et la configuration de l'AWS Command Line Interface dans le Guide de l'utilisateur AWS Command Line Interface.

1. Dans un éditeur de texte, créez un fichier. Collez le contenu suivant dans l'éditeur :

```
{
  "TemplateName": "SampleTemplate",
  "FromEmailAddress": "sender@example.com",
  "TemplateSubject": "Please confirm your email address",
  "TemplateContent": "<html>
```

```
                        <head></head>
                        <body style='font-family:sans-serif;'>
                          <h1 style='text-align:center'>Ready to start sending
                          email with ProductName?</h1>
                          <p>We here at Example Corp are happy to have you on
                            board! There's just one last step to complete before
                            you can start sending email. Just click the following
                            link to verify your email address. Once we confirm that
                            you're really you, we'll give you some additional
                            information to help you get started with ProductName.</p>
                        </body>
                        </html>",
  "SuccessRedirectionURL": "https://www.example.com/verifysuccess",
  "FailureRedirectionURL": "https://www.example.com/verifyfailure"
}
```

> **Important**
>
> Pour faciliter la lecture de l'exemple précédent, l'attribut `TemplateContent` contient des sauts de ligne. Si vous collez l'exemple précédent dans votre fichier texte, supprimez les sauts de ligne avant de continuer.

Remplacez les valeurs de `TemplateName`, `FromEmailAddress`, `TemplateSubject`, `TemplateContent`, `SuccessRedirectionURL` et `FailureRedirectionURL` par vos propres valeurs.

> **Note**
>
> L'adresse e-mail que vous spécifiez pour le paramètre `FromEmailAddress` doit être vérifiée, ou doit être une adresse sur un domaine vérifié. Pour plus d'informations, consultez Identités vérifiées dans Amazon SES.

Lorsque vous avez terminé, enregistrez le fichier sous `customverificationemail.json`.

2. Sur la ligne de commande, entrez la commande suivante pour créer le modèle d'e-mail de vérification personnalisé :

```
aws sesv2 create-custom-verification-email-template --cli-input-json file://
customverificationemail.json
```

3. (Facultatif) Si vous le souhaitez, vous pouvez confirmer que le modèle a été créé en entrant la commande suivante :

```
aws sesv2 list-custom-verification-email-templates
```

Modification d'un modèle d'e-mail de vérification personnalisé

Vous pouvez modifier un modèle d'e-mail de vérification personnalisé à l'aide de l'opération `UpdateCustomVerificationEmailTemplate`. Cette opération accepte les mêmes entrées que l'opération `CreateCustomVerificationEmailTemplate` (c'est-à-dire, les attributs `TemplateName`, `FromEmailAddress`, `TemplateSubject`, `TemplateContent`, `SuccessRedirectionURL` et `FailureRedirectionURL`). Toutefois, avec l'opération `UpdateCustomVerificationEmailTemplate`, aucun de ces attributs n'est obligatoire. Lorsque vous transmettez une valeur pour `TemplateName` identique au nom d'un modèle d'e-mail de vérification personnalisé, les attributs que vous spécifiez remplacent les attributs initiaux du modèle.

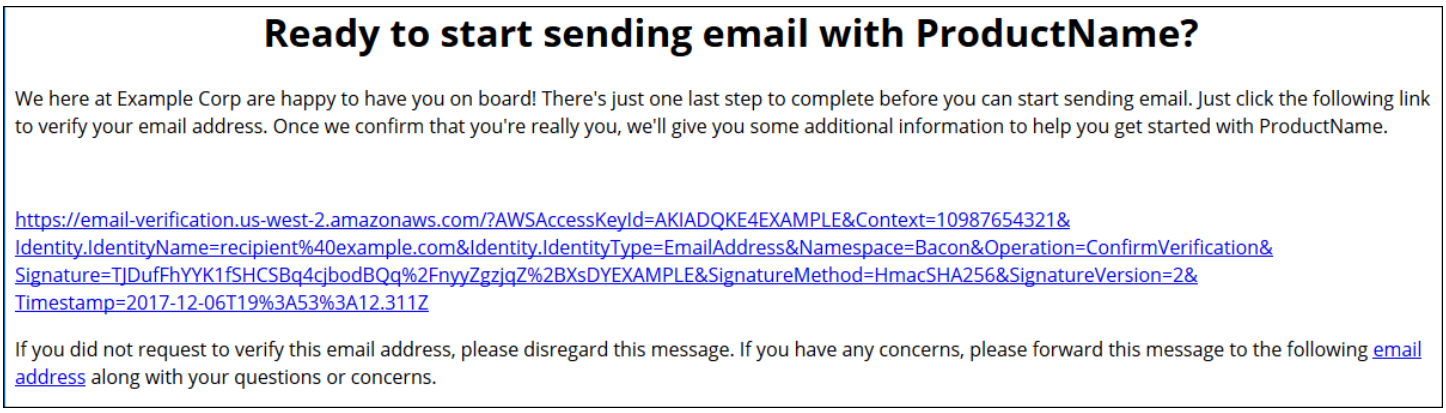
Envoi d'e-mails de vérification à l'aide de modèles personnalisés

Une fois que vous avez créé au moins un modèle d'e-mail de vérification personnalisé, vous pouvez l'envoyer à vos clients en appelant l'opération d'API SendCustomVerificationEmail. Vous pouvez appeler l'opération `SendCustomVerificationEmail` en utilisant l'un des kits SDK AWS ou l'AWS CLI. L'opération `SendCustomVerificationEmail` utilise les entrées suivantes :

Attribut	Description
`EmailAddress`	Adresse e-mail faisant l'objet de la vérification.
`TemplateName`	Nom du modèle d'e-mail de vérification personnalisé envoyé à l'adresse e-mail faisant l'objet de la vérification.
`ConfigurationSetName`	(Facultatif) Nom d'un jeu de configurations à utiliser lors de l'envoi de l'e-mail de vérification.

Par exemple, supposons que vos clients s'inscrivent à votre service en utilisant un formulaire de votre application. Lorsque le client a rempli et envoyé le formulaire, votre application appelle l'opération `SendCustomVerificationEmail` en transmettant l'adresse e-mail du client et le nom du modèle que vous souhaitez utiliser.

Votre client reçoit un e-mail qui utilise le modèle d'e-mail personnalisé que vous avez créé. Amazon SES ajoute automatiquement un lien unique vers le destinataire, ainsi qu'une courte clause de non-responsabilité. L'image suivante illustre un exemple d'e-mail de vérification qui utilise le modèle créé dans Création d'un modèle d'e-mail de vérification personnalisé.



Ready to start sending email with ProductName?

We here at Example Corp are happy to have you on board! There's just one last step to complete before you can start sending email. Just click the following link to verify your email address. Once we confirm that you're really you, we'll give you some additional information to help you get started with ProductName.

https://email-verification.us-west-2.amazonaws.com/?AWSAccessKeyId=AKIADQKE4EXAMPLE&Context=10987654321&Identity.IdentityName=recipient%40example.com&Identity.IdentityType=EmailAddress&Namespace=Bacon&Operation=ConfirmVerification&Signature=TJDufFhYYK1fSHCSBq4cjbodBQq%2FnyyZgzjqZ%2BXsDYEXAMPLE&SignatureMethod=HmacSHA256&SignatureVersion=2&Timestamp=2017-12-06T19%3A53%3A12.311Z

If you did not request to verify this email address, please disregard this message. If you have any concerns, please forward this message to the following email address along with your questions or concerns.

Questions fréquentes sur l'e-mail de vérification personnalisé

Cette section contient les réponses aux questions fréquentes sur la fonction de modèle d'e-mail de vérification personnalisé.

Q1. Combien de modèles d'e-mail de vérification personnalisé puis-je créer ?

Vous pouvez créer jusqu'à 50 modèles d'e-mail de vérification personnalisé par compte Amazon SES.

Q2. Sous quelle forme les e-mails de vérification personnalisés apparaissent-ils aux destinataires ?

Les e-mails de vérification personnalisés incluent le contenu que vous avez spécifié lors de la création du modèle, suivi d'un lien sur lequel les destinataires doivent cliquer pour vérifier leurs adresses e-mail.

Q3. Puis-je afficher un aperçu de l'e-mail de vérification personnalisé ?

Pour afficher l'aperçu d'un e-mail de vérification personnalisé, utilisez l'opération `SendCustomVerificationEmail` pour envoyer un e-mail de vérification à l'une de vos adresses. Si vous ne cliquez pas sur le lien de vérification, Amazon SES ne crée pas d'identité. Si vous cliquez

sur le lien de vérification, vous pouvez, si vous le souhaitez, supprimer la nouvelle identité créée à l'aide de l'opération `DeleteIdentity`.

Q4. Puis-je inclure des images dans mes modèles d'e-mail de vérification personnalisé ?

Vous pouvez intégrer des images dans le code HTML de vos modèles, en utilisant l'encodage en base64. Lorsque vous intégrez des images de cette manière, Amazon SES les convertit automatiquement en pièces jointes. Vous pouvez encoder une image à partir de la ligne de commande en entrant l'une des commandes suivantes :

Linux, macOS, or Unix

```
base64 -i imagefile.png | tr -d '\n' > output.txt
```

Windows

```
certutil -encodehex -f imagefile.png output.txt 0x40000001
```

Remplacez *`imagefile.png`* par le nom du fichier que vous souhaitez encoder. Dans les deux commandes ci-dessus, l'image encodée en base64 est enregistrée dans `output.txt`.

Vous pouvez intégrer l'image encodée en base64 en incluant les éléments suivants dans le code HTML pour le modèle : `<img src="`*`base64EncodedImage`*`"/>`

Dans l'exemple ci-dessus, remplacez *`png`* par le type de fichier de l'image encodée (par exemple, .jpg ou .gif) et remplacez *`base64EncodedImage`* par l'image encodée en base64 (c'est-à-dire, le contenu de `output.txt` résultant de l'une des commandes précédentes).

Q5. Y a-t-il des limitations pour le contenu que je peux inclure dans les modèles d'e-mail de vérification personnalisé ?

La taille des modèles d'e-mail de vérification personnalisé ne doit pas dépasser 10 Mo. De plus, les modèles d'e-mail de vérification personnalisé contenant du code HTML peuvent utiliser uniquement les balises et les attributs répertoriés dans le tableau suivant :

Balise HTML	Attributs autorisés
`abbr`	`class, id, style, title`

Balise HTML	Attributs autorisés
acronym	class, id, style, title
address	class, id, style, title
area	class, id, style, title
b	class, id, style, title
bdo	class, id, style, title
big	class, id, style, title
blockquote	cite, class, id, style, title
body	class, id, style, title
br	class, id, style, title
button	class, id, style, title
caption	class, id, style, title
center	class, id, style, title
cite	class, id, style, title
code	class, id, style, title
col	class, id, span, style, title, width
colgroup	class, id, span, style, title, width
dd	class, id, style, title
del	class, id, style, title
dfn	class, id, style, title

Balise HTML	Attributs autorisés
dir	class, id, style, title
div	class, id, style, title
dl	class, id, style, title
dt	class, id, style, title
em	class, id, style, title
fieldset	class, id, style, title
font	class, id, style, title
form	class, id, style, title
h1	class, id, style, title
h2	class, id, style, title
h3	class, id, style, title
h4	class, id, style, title
h5	class, id, style, title
h6	class, id, style, title
head	class, id, style, title
hr	class, id, style, title
html	class, id, style, title
i	class, id, style, title
img	align, alt, class, height, id, src, style, title, width
input	class, id, style, title

Balise HTML	Attributs autorisés
ins	class, id, style, title
kbd	class, id, style, title
label	class, id, style, title
legend	class, id, style, title
li	class, id, style, title
map	class, id, style, title
menu	class, id, style, title
ol	class, id, start, style, title, type
optgroup	class, id, style, title
option	class, id, style, title
p	class, id, style, title
pre	class, id, style, title
q	cite, class, id, style, title
s	class, id, style, title
samp	class, id, style, title
select	class, id, style, title
small	class, id, style, title
span	class, id, style, title
strike	class, id, style, title
strong	class, id, style, title

Balise HTML	Attributs autorisés
sub	class, id, style, title
sup	class, id, style, title
table	class, id, style, summary, title, width
tbody	class, id, style, title
td	abbr, axis, class, colspan, id, rowspan, style, title, width
textarea	class, id, style, title
tfoot	class, id, style, title
th	abbr, axis, class, colspan, id, rowspan, scope, style, title, width
thead	class, id, style, title
tr	class, id, style, title
tt	class, id, style, title
u	class, id, style, title
ul	class, id, style, title, type
var	class, id, style, title

> **Note**
>
> Les modèles d'e-mail de vérification personnalisé ne doivent pas inclure d'étiquette de commentaire.

Q6. Combien d'adresses e-mail vérifiées mon compte peut-il contenir ?

Votre compte Amazon SES peut avoir jusqu'à 10 000 identités vérifiées dans chaque région AWS. Dans Amazon SES, les identités comprennent à la fois des domaines et des adresses e-mail vérifiés.

Q7. Puis-je créer des modèles d'e-mail de vérification personnalisé à l'aide de la console Amazon SES ?

Actuellement, il est possible de créer, modifier et supprimer des e-mails de vérification personnalisés seulement à l'aide de l'API Amazon SES.

Q8. Puis-je suivre les événements d'ouvertures et de clics qui se produisent lorsque les clients reçoivent des e-mails de vérification personnalisés ?

Les e-mails de vérification personnalisés ne peuvent pas inclure le suivi d'ouvertures et de clics.

Q9. Les e-mails de vérification personnalisés peuvent-ils inclure des en-têtes personnalisés ?

Les e-mails de vérification personnalisés ne peuvent pas inclure d'en-tête personnalisé.

Q10. Puis-je supprimer le texte qui s'affiche au bas des e-mails de vérification personnalisés ?

Le texte suivant est automatiquement ajouté à la fin de chaque e-mail de vérification personnalisé et ne peut pas être supprimé :

Si vous n’avez pas demandé à vérifier cette adresse e-mail, veuillez ignorer ce message.

Q11. Les e-mails de vérification personnalisés sont-ils signés par DKIM ?

Pour que les e-mails de vérification soient signés par DKIM, l'adresse e-mail que vous indiquez dans l'attribut `FromEmailAddress` lors de la création du modèle d'e-mail de vérification doit être configurée pour générer une signature DKIM. Pour en savoir plus sur la configuration de DKIM pour les domaines et les adresses e-mail, consultez the section called “Authentification d'e-mails avec DKIM”.

Q12. Pourquoi les opérations d'API du modèle d'e-mail de vérification personnalisé s'affichent-elles dans le kit SDK ou de la CLI ?

Si vous ne parvenez pas à utiliser les opérations du modèle d'e-mail de vérification personnalisé dans un kit SDK ou l'AWS CLI, il se peut que vous utilisiez une version antérieure du kit SDK ou de la CLI. Les opérations du modèle d'e-mail de vérification personnalisé sont disponibles dans les kits SDK et les interfaces de ligne de commande suivants :

- Version 1.14.6 ou ultérieure de l' AWS Command Line Interface
- Version 3.3.205.0 ou ultérieure de AWS SDK for .NET
- Version 1.3.20170531.19 ou ultérieure du kit SDK AWS pour C++
- Version 1.12.43 ou ultérieure de AWS SDK for Go
- Version 1.11.245 ou ultérieure de AWS SDK for Java
- Version 2.166.0 ou ultérieure de AWS SDK for JavaScript
- Version 3.45.2 ou ultérieure de AWS SDK for PHP
- Version 1.5.1 ou ultérieure de AWS SDK for Python (Boto)
- Version 1.5.0 ou ultérieure de la gem `aws-sdk-ses` dans AWS SDK for Ruby

Q13. Pourquoi est-ce que je reçois des erreurs **`ProductionAccessNotGranted`** lorsque j'envoie des e-mails de vérification personnalisés ?

L'erreur `ProductionAccessNotGranted` indique que votre compte est toujours dans l'environnement de test (sandbox) Amazon SES. Vous pouvez uniquement envoyer des e-mails de vérification personnalisés si votre compte a été supprimé de l'environnement de test (sandbox). Pour plus d'informations, consultez Demande d'accès à la production (sortie du sandbox d'Amazon SES).

Vérification des identités dans Amazon SES

Dans la console Amazon SES, vous pouvez afficher une liste d'identités, ouvrir une identité pour afficher et modifier ses paramètres, associer un jeu de configurations par défaut, ou supprimer une ou plusieurs identités.

> **Note**
>
> Les procédures décrites dans cette section ne s'appliquent qu'aux identités dans la Région AWS sélectionnée. Pour gérer les identités qui ont été créées dans différentes régions, répétez les procédures pour chaque Région AWS.

Affichage d'une liste d'identités dans Amazon SES

Vous pouvez utiliser la console Amazon SES ou l'API pour afficher une liste d'identités de domaine et d'adresse e-mail qui ont été vérifiées ou qui sont en cours de vérification. Vous pouvez également afficher les identifiants pour lesquels la vérification a échoué.

Pour afficher les identités de votre domaine et de votre adresse e-mail (console)

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans la console, utilisez le sélecteur de région afin de choisir la Région AWS pour laquelle vous souhaitez afficher votre liste d'identités.

   > **Note**
   >
   > Cette procédure n'affiche qu'une liste d'identités pour la Région AWS sélectionnée.

3. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées). La table Loaded identities (Identités chargées) affiche à la fois les identités de domaine et d'adresse e-mail. La colonne Status (État) indique si une identité a été vérifiée, est en attente de vérification ou si le processus de vérification a échoué. Les définitions de toutes les valeurs d'état sont les suivantes :

   - Vérified (Vérifié) : l'envoi de votre identité dans SES a été vérifiée.
   - Failure (Échec) : SES n'a pas pu vérifier votre identité. Dans le cas d'un domaine, cela signifie que SES n'est pas parvenu à détecter les enregistrements DNS dans les 72 heures. S'il s'agit d'une adresse e-mail, l'e-mail de vérification qui lui a été envoyé n'a pas été reconnu dans les 24 heures.
   - Pending (En attente) : SES tente toujours de vérifier l'identité.
   - Temporary Failure (Échec temporaire) : dans le cas d'un domaine vérifié précédemment, SES recherchera périodiquement l'enregistrement DNS nécessaire à la vérification. Si, à un moment donné, SES ne parvient pas à détecter cet enregistrement, l'état passe à Temporary Failure (Échec temporaire). SES cherchera à nouveau l'enregistrement DNS pendant 72 heures. S'il ne parvient pas à le détecter, l'état du domaine passe à Failure (Échec). S'il détecte l'enregistrement, l'état du domaine passe à Verified (Vérifié).
   - Not started (Non démarré) : vous n'avez pas encore lancé le processus de vérification.

4. Pour trier les identités en fonction du statut de vérification, choisissez la colonne Status (État).
5. Pour afficher la page de détails d'une identité, sélectionnez l'identité que vous souhaitez afficher.

Suppression d'une identité dans Amazon SES

Vous pouvez utiliser la console ou l'API Amazon SES pour supprimer une identité de domaine ou d'adresse e-mail de votre compte dans la sélectionnée Région AWS.

Pour supprimer une identité de domaine ou d'adresse e-mail (console)

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans la console, utilisez le sélecteur de région afin de choisir la Région AWS pour laquelle vous souhaitez supprimer une ou plusieurs identités.
3. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).

   La table Loaded identities (Identités chargées) affiche la liste des identités de domaine et d'adresse e-mail.
4. Dans la colonne Identité (Identity) sélectionnez l'identité que vous souhaitez supprimer. Vous pouvez supprimer plusieurs identités en cochant la case à côté de chaque identité que vous souhaitez supprimer.
5. Sélectionnez Delete.

Modification d'une identité existante dans Amazon SES

Vous pouvez utiliser la console ou l'API Amazon SES pour modifier une identité de domaine ou d'adresse e-mail de votre compte dans la sélectionnée Région AWS.

Pour modifier une identité de domaine ou d'adresse e-mail (console)

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans la console, utilisez le sélecteur de région afin de choisir la Région AWS pour laquelle vous souhaitez modifier une ou plusieurs identités.
3. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).

   La table Loaded identities (Identités chargées) affiche la liste des identités de domaine et d'adresse e-mail.

4. Dans la colonne Identity (Identité), sélectionnez l'identité que vous souhaitez modifier (en cliquant directement sur le nom de l'identité plutôt que sur sa case à cocher).
5. Sur la page détaillée de l'identité, sélectionnez l'onglet contenant les catégories que vous souhaitez modifier.
6. Dans l'un des conteneurs catégoriques de l'onglet sélectionné, choisissez le bouton Edit (Modifier) de l'attribut que vous souhaitez modifier, apportez vos modifications, puis choisissez Save changes (Enregistrer les modifications).

    a. Si vous souhaitez modifier des attributs sous l'onglet Authentication (Authentification), que votre identité de domaine est hébergée dans Amazon Route 53 et que vous n'avez pas encore publié ses enregistrements DNS, il y aura un bouton Publish DNS records to Route53 (Publier des enregistrements DNS sur Route53) (à côté du bouton Edit (Modifier)) dans l'un ou l'autre ou les deux conteneurs DomainKeys Identified Mail (DKIM) ou Custom MAIL FROM domain (Domaine MAIL FROM personnalisé).

    > **Note**
    >
    > L'onglet Authentication (Authentification) n'est présent que lorsque votre compte possède un domaine vérifié ou une adresse e-mail utilisant un domaine vérifié dans votre compte.

    b. Vous pouvez publier les enregistrements DNS directement depuis le bouton Publish DNS records to Route53 (Publier des enregistrements DNS sur Route53) : il suffit de cliquer dessus, une bannière de confirmation s'affichera et le bouton Publish DNS records to Route53 (Publier des enregistrements DNS sur Route53) ne sera plus visible pour le conteneur respectif.
7. Répétez les étapes 5 et 6 pour chaque attribut de l'identité que vous souhaitez modifier.

Modifier une identité pour utiliser un jeu de configuration par défaut à l'aide de l'API

Vous pouvez utiliser l'opération PutEmailIdentityConfigurationSetAttributes pour ajouter ou supprimer un jeu de configurations par défaut d'une identité d'adresse e-mail existante.

> **Note**
>
> Avant d'effectuer la procédure complète décrite dans cette section, vous devez installer et configurer l' AWS CLI. Pour en savoir plus, veuillez consulter le Guide de l'utilisateur AWS Command Line Interface.

Pour ajouter un ensemble de configurations par défaut à l'aide de la AWS CLI

- Sur la ligne de commande, saisissez la commande suivante pour utiliser l'opération PutEmailIdentityConfigurationSetAttributes.

```
aws sesv2 put-email-identity-configuration-set-attributes --email-identity ADDRESS-OR-DOMAIN --configuration-set-name CONFIG-SET
```

Dans les commandes précédentes, remplacez *ADDRESS-OR-DOMAIN* par l'identité d'adresse e-mail que vous souhaitez vérifier. Remplacez *CONFIG-SET* par le nom du jeu de configurations que vous souhaitez définir comme jeu de configurations par défaut de l'identité.

Si la commande s'exécute correctement, elle se termine sans fournir de sortie.

Pour éliminer un ensemble de configurations par défaut à l'aide de la AWS CLI

- Sur la ligne de commande, saisissez la commande suivante pour utiliser l'opération PutEmailIdentityConfigurationSetAttributes.

```
aws sesv2 put-email-identity-configuration-set-attributes --email-identity ADDRESS-OR-DOMAIN
```

Dans les commandes précédentes, remplacez *ADDRESS-OR-DOMAIN* par l'identité d'adresse e-mail que vous souhaitez vérifier.

Si la commande s'exécute correctement, elle se termine sans fournir de sortie.

Récupérer le jeu de configurations par défaut utilisé par l'identité (API)

Vous pouvez utiliser l'opération GetEmailIdentity pour renvoyer le jeu de configurations par défaut d'une identité d'adresse e-mail, le cas échéant.

> **Note**
>
> Avant d'effectuer la procédure complète décrite dans cette section, vous devez installer et configurer l' AWS CLI. Pour en savoir plus, veuillez consulter le Guide de l'utilisateur AWS Command Line Interface.

Pour retourner un ensemble de configurations par défaut à l'aide de la AWS CLI

- Sur la ligne de commande, saisissez la commande suivante pour utiliser l'opération GetEmailIdentity.

```
aws sesv2 get-email-identity --email-identity ADDRESS-OR-DOMAIN
```

Dans les commandes précédentes, remplacez *ADDRESS-OR-DOMAIN* par l'identité d'adresse e-mail pour laquelle vous souhaitez connaître le jeu de configurations par défaut, le cas échéant.

Si la commande s'exécute correctement, elle fournit à un objet JSON les détails de l'identité d'adresse e-mail.

Remplacer le jeu de configurations par défaut actuel utilisé par l'identité (API)

Vous pouvez utiliser l'opération SendEmail pour envoyer des e-mails avec un jeu de configurations différent. Si vous le faites, le jeu de configurations que vous spécifiez remplace le jeu de configurations par défaut de l'identité.

> **Note**
>
> Avant d'effectuer la procédure complète décrite dans cette section, vous devez installer et configurer l' AWS CLI. Pour en savoir plus, veuillez consulter le Guide de l'utilisateur AWS Command Line Interface.

Pour remplacer un ensemble de configurations par défaut à l'aide de la AWS CLI

- Sur la ligne de commande, saisissez la commande suivante pour utiliser l'opération SendEmail.

```
aws sesv2 send-email --destination file://DESTINATION-JSON --content file://CONTENT-
JSON --from-email-address ADDRESS-OR-DOMAIN --configuration-set-name CONFIG-SET
```

Dans les commandes précédentes, remplacez *DESTINATION-JSON* par votre fichier JSON de destination, *CONTENT-JSON* par votre fichier JSON de contenu, *ADDRESS-OR-DOMAIN* par votre adresse e-mail FROM et *CONFIG-SET* par le nom du jeu de configurations que vous souhaitez utiliser au lieu du jeu de configurations par défaut pour l'identité.

Si la commande s'exécute correctement, elle génère un `MessageId`.

Configuration des identités dans Amazon SES

Amazon Simple Email Service (Amazon SES) utilise le protocole SMTP (Simple Mail Transfer Protocol) pour envoyer des e-mails. Étant donné que le protocole SMTP ne fournit aucune authentification par lui-même, les expéditeurs de courrier indésirable peuvent envoyer des messages électroniques qui prétendent provenir d'une autre personne, tout en masquant leur origine réelle. En falsifiant les en-têtes d'e-mail et en usurpant les adresses IP source, les expéditeurs de courrier indésirable peuvent amener les destinataires des messages à croire que ces derniers sont authentiques.

La plupart des ISP qui assurent le trafic d'e-mails prennent des mesures pour en évaluer l'authenticité. Une de ces mesures prises par les ISP consiste à déterminer si un e-mail est authentifié. L'authentification nécessite que les expéditeurs confirment qu'ils sont bien propriétaires du compte depuis lequel ils envoient le message. Dans certains cas, les ISP refusent de transférer un e-mail qui n'est pas authentifié. Pour garantir une délivrabilité optimale, nous vous recommandons d'authentifier vos e-mails.

Les sections suivantes décrivent deux mécanismes d'authentification utilisés par les FAI, les normes SPF (Sender Policy Framework) et norme DKIM (DomainKeys Identified Mail), et fournissent des instructions sur la façon d'utiliser ces normes avec Amazon SES.

- Pour en savoir plus sur le standard SPF, qui fournit une manière de tracer un message électronique jusqu'au système à partir duquel il a été envoyé, consultez Authentification d'e-mails avec SPF dans Amazon SES.
- Pour en savoir plus sur le standard DKIM, qui permet de signer vos e-mails de manière à montrer aux ISP que vos messages sont légitimes et qu'ils n'ont pas été modifiés en transit, consultez Authentification d'e-mails avec DKIM dans Amazon SES.

- Pour savoir comment vous conformer à la spécification DMARC (Domain-based Message Authentication, Reporting and Conformance), qui repose sur les normes SPF et DKIM, consultez Mise en conformité au protocole d'authentification DMARC dans Amazon SES.

Méthodes d'authentification d'e-mail

Amazon Simple Email Service (Amazon SES) utilise le protocole SMTP (Simple Mail Transfer Protocol) pour envoyer des e-mails. Étant donné que le protocole SMTP ne fournit aucune authentification par lui-même, les expéditeurs de courrier indésirable peuvent envoyer des messages électroniques qui prétendent provenir d'une autre personne, tout en masquant leur origine réelle. En falsifiant les en-têtes d'e-mail et en usurpant les adresses IP source, les expéditeurs de courrier indésirable peuvent amener les destinataires des messages à croire que ces derniers sont authentiques.

La plupart des ISP qui assurent le trafic d'e-mails prennent des mesures pour en évaluer l'authenticité. Une de ces mesures prises par les ISP consiste à déterminer si un e-mail est authentifié. L'authentification nécessite que les expéditeurs confirment qu'ils sont bien propriétaires du compte depuis lequel ils envoient le message. Dans certains cas, les ISP refusent de transférer un e-mail qui n'est pas authentifié. Pour garantir une délivrabilité optimale, nous vous recommandons d'authentifier vos e-mails.

Table des matières

Authentification d'e-mails avec DKIM dans Amazon SES

norme DKIM (DomainKeys Identified Mail)(DKIM) est un standard de sécurité conçue pour garantir qu'un e-mail censé provenir d'un domaine spécifique a bien été autorisé par le propriétaire de ce domaine. Elle utilise le chiffrement de clé publique pour signer un e-mail avec une clé privée. Les serveurs de destinataires peuvent ensuite utiliser une clé publique publiée dans le DNS d'un domaine pour vérifier que certaines parties de l'e-mail n'ont pas été modifiées pendant le transit.

Les signatures DKIM sont facultatives. Vous pouvez décider de signer vos e-mails à l'aide d'une signature DKIM pour améliorer la délivrabilité avec les fournisseurs de messagerie compatibles avec le standard DKIM. Amazon SES propose trois options pour signer vos messages à l'aide d'une signature DKIM :

- Easy DKIM : SES génère une paire de clés public/privé et ajoute automatiquement une signature DKIM à chaque message que vous envoyez à partir de cette identité, consultez Easy DKIM dans Amazon SES.
- BYODKIM (Bring Your Own DKIM) : vous fournissez votre propre paire de clés public/privé et SES ajoute une signature DKIM à chaque message que vous envoyez à partir de cette identité, consultez Fournissez votre propre jeton d'authentification DKIM (BYODKIM) dans Amazon SES.
- Ajouter manuellement la signature DKIM : vous ajoutez votre propre signature DKIM à tous les e-mails que vous envoyez à l'aide de l'API `SendRawEmail`, consultez Signature DKIM manuelle dans Amazon SES.

Longueur de la clé DKIM

Puisque de nombreux fournisseurs de DNS prennent désormais en charge le cryptage RSA 2048 bits de DKIM, Amazon SES prend également en charge DKIM 2048 pour permettre une authentification plus sûre des e-mails et l'utilise donc en tant que longueur de clé par défaut lorsque vous configurez Easy DKIM à partir de l'API ou de la console. Les clés de 2048 bits peuvent être configurées et utilisées dans Bring Your Own DKIM (BYODKIM) également, où la longueur de votre clé de signature doit être au moins de 1024 bits et pas plus de 2048 bits.

Pour des raisons de sécurité et de délivrabilité de votre e-mail, lorsque vous configurez Easy DKIM, vous avez le choix d'utiliser des longueurs de clé de 1024 ou 2048 bits, avec la possibilité de revenir à 1024 en cas de problèmes liés à des fournisseurs DNS qui ne prennent pas encore en charge 2048. Lorsque vous créez une nouvelle identité, elle est créée avec DKIM 2048 par défaut, sauf si vous spécifiez 1024.

Pour préserver la délivrabilité des e-mails en transit, il existe des restrictions quant à la fréquence à laquelle vous pouvez modifier la longueur de la clé DKIM. Les restrictions sont les suivantes :

- Impossibilité de passer à la même longueur de clé que celle déjà configurée.
- Impossibilité de passer à une longueur de clé différente plus d'une fois au cours d'une période de 24 heures (sauf s'il s'agit de la première rétrogradation à 1024 de cette période).

Lorsque votre e-mail est en transit, DNS utilise votre clé publique pour l'authentifier. Par conséquent, si vous changez de clé trop rapidement ou trop fréquemment, DNS peut ne pas être en mesure d'authentifier votre e-mail par DKIM, car l'ancienne clé peut déjà avoir été annulée.

Considérations relatives à DKIM

Lorsque vous utilisez DKIM pour authentifier vos e-mails, les règles suivantes s'appliquent :

- Vous devez uniquement configurer DKIM pour le domaine que vous utilisez dans votre adresse « From ». Vous n'avez pas besoin de configurer DKIM pour les domaines que vous utilisez dans les adresses « Return-Path » (Chemin de retour) ou « Reply-to » (Répondre à).
- Amazon SES est disponible dans plusieurs régions AWS. Si vous utilisez plusieurs Régions AWS pour envoyer des e-mails, vous devez exécuter le processus de configuration de DKIM dans chacune de ces Régions pour vous assurer que tous vos e-mails sont signés par DKIM.
- Étant donné que les propriétés DKIM sont héritées du domaine parent, lorsque vous vérifiez un domaine avec l'authentification DKIM :
  - L'authentification DKIM s'appliquera également à tous les sous-domaines de ce domaine.
    - Les paramètres DKIM d'un sous-domaine peuvent remplacer ceux du domaine parent via la désactivation de l'héritage, si vous ne souhaitez pas que le sous-domaine utilise l'authentification DKIM. Vous avez la possibilité de le réactiver ultérieurement.
  - L'authentification DKIM s'appliquera également à tous les e-mails envoyés à partir d'une identité e-mail faisant référence au domaine vérifié DKIM dans son adresse.
    - Les paramètres DKIM d'une adresse e-mail peuvent remplacer ceux du sous-domaine (le cas échéant) et du domaine parent via la désactivation de l'héritage, si vous souhaitez envoyer des e-mails sans authentification DKIM. Vous avez la possibilité de le réactiver ultérieurement.

Comprendre les propriétés de signature DKIM héritées

Il est important de comprendre d'abord qu'une identité d'adresse e-mail hérite de ses propriétés de signature DKIM de son domaine parent si ce domaine a été configuré avec DKIM, indépendamment du fait que Easy DKIM ou BYODKIM ait été utilisé. Par conséquent, la désactivation ou l'activation de la signature DKIM sur l'identité de l'adresse e-mail remplace les propriétés de signature DKIM du domaine sur la base de ces éléments clés :

- Si vous avez déjà configuré DKIM pour le domaine auquel appartient une adresse e-mail, vous n'avez pas besoin d'activer la signature DKIM pour l'identité de l'adresse e-mail également.

- Lorsque vous configurez DKIM pour un domaine, Amazon SES authentifie automatiquement chaque e-mail provenant de chaque adresse de ce domaine grâce aux propriétés DKIM héritées du domaine parent.
- Les paramètres DKIM pour une identité d'adresse e-mail spécifique remplacent automatiquement les paramètres du domaine ou du sous-domaine parent (le cas échéant) auquel l'adresse appartient.

Étant donné que les propriétés de signature DKIM de l'identité d'adresse e-mail sont héritées du domaine parent, si vous envisagez de remplacer ces propriétés, vous devez garder à l'esprit les règles hiérarchiques de remplacement, comme expliqué dans le tableau ci-dessous.

La signature DKIM n'est pas activée dans le domaine parent	La signature DKIM est activée dans le domaine parent
Vous ne pouvez pas activer la signature DKIM sur l'identité de l'adresse e-mail.	Vous pouvez désactiver la signature DKIM sur l'identité de l'adresse e-mail.
	Vous pouvez réactiver la signature DKIM sur l'identité de l'adresse e-mail.

Il n'est généralement pas recommandé de désactiver la signature DKIM, car cela risque de ternir la réputation de l'expéditeur et d'augmenter le risque de voir les e-mails que vous envoyez aboutir dans les dossiers de courrier indésirable ou de spam, ou de voir votre domaine usurpé.

Toutefois, il existe la possibilité de remplacer les propriétés de signature DKIM héritées du domaine sur une identité d'adresse e-mail pour tout cas d'utilisation particulier ou décision commerciale externe pour lesquels vous pourriez avoir à désactiver la signature DKIM de façon permanente ou temporaire, ou à la réactiver ultérieurement. Consultez the section called “Remplacement de la signature DKIM sur l'adresse e-mail”.

Easy DKIM dans Amazon SES

Lorsque vous configurez la fonction Easy DKIM pour une identité de domaine, Amazon SES ajoute automatiquement une clé DKIM 2 048 bits à chaque e-mail que vous envoyez à partir de cette identité. Vous pouvez configurer Easy DKIM à l'aide de la console Amazon SES ou de l'API.

> **Note**
>
> Pour configurer Easy DKIM, vous devez modifier les paramètres DNS de votre domaine. Si vous utilisez Route 53 comme votre fournisseur DNS, Amazon SES peut créer automatiquement les registres appropriés pour vous. Si vous utilisez un autre fournisseur DNS, consultez la documentation de ce dernier pour en savoir plus sur la modification des paramètres DNS pour votre domaine.

> **Warning**
>
> Si BYODKIM est actuellement activé et que vous passez à Easy DKIM, sachez qu'Amazon SES n'utilisera pas BYODKIM pour signer vos e-mails pendant la configuration d'Easy DKIM et que votre statut DKIM est en attente. Entre le moment où vous passez l'appel pour activer Easy DKIM (via l'API ou la console) et le moment où SES peut confirmer votre configuration DNS, vos e-mails peuvent être envoyés par SES sans signature DKIM. Par conséquent, il est conseillé d'utiliser une étape intermédiaire pour migrer d'une méthode de signature DKIM à l'autre (par exemple, en utilisant un sous-domaine de votre domaine avec BYODKIM activé, puis en le supprimant une fois la vérification Easy DKIM passée), ou d'effectuer cette activité pendant les temps d'arrêt de votre application, le cas échéant.

Configuration de Easy DKIM pour une identité de domaine vérifiée

La procédure de cette section est simplifiée afin de présenter uniquement les étapes nécessaires pour configurer Easy DKIM sur une identité de domaine que vous avez déjà créée. Si vous n'avez pas encore créé d'identité de domaine ou si vous souhaitez voir toutes les options disponibles pour personnaliser une identité de domaine, telles que l'utilisation d'un jeu de configuration par défaut, d'un domaine MAIL FROM personnalisé et d'étiquettes, veuillez consulter the section called “Création d'une identité de domaine”.

Une partie de la création d'une identité de domaine Easy DKIM consiste à configurer sa vérification basée sur DKIM. Vous aurez donc le choix d'accepter la valeur par défaut Amazon SES de 2 048 bits, ou de la remplacer en sélectionnant 1 024 bits. Voir the section called “Longueur de la clé DKIM” pour en savoir plus sur les longueurs de clés de signature DKIM et sur la façon de les modifier.

Pour configurer Easy DKIM pour un domaine

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).
3. Dans la liste des identités, choisissez une identité dans laquelle le type d'identité est le Domaine.

   > **Note**
   >
   > Si vous devez créer ou vérifier un domaine, veuillez consulter Création d'une identité de domaine.

4. Sous l'onglet Authentification, dans le conteneur norme DKIM (DomainKeys Identified Mail), choisissez Edit (Modifier).
5. Dans le conteneur Advanced DKIM settings (Paramètres avancés de DKIM), choisissez le bouton Easy DKIM dans la zoneIdentity type (Type d'identité).
6. Dans DKIM signing key length (Longueur de clé de signature DKIM), choisissez RSA_2048_BIT ou RSA_1024_BIT.
7. Dans DKIM signatures (Signatures DKIM), cochez la case Enabled (Activé).
8. Choisissez Enregistrer les modifications.
9. Maintenant que vous avez configuré votre identité de domaine avec Easy DKIM, vous devez terminer le processus de vérification avec votre fournisseur DNS. Passez à the section called “Vérification d'une identité de domaine” et suivez les procédures d'authentification DNS pour Easy DKIM.

Modifier la longueur de la clé de signature Easy DKIM pour une identité

La procédure décrite dans cette section montre comment vous pouvez facilement modifier les bits Easy DKIM requis pour l'algorithme de signature. Bien qu'une longueur de signature de 2048 bits soit préférable pour le niveau de sécurité qu'elle procure, certaines situations peuvent vous obliger à utiliser la longueur de 1024 bits, par exemple si vous devez utiliser un fournisseur DNS qui ne prend en charge que DKIM 1024.

Pour préserver la délivrabilité des e-mails en transit, il existe des restrictions quant à la fréquence à laquelle vous pouvez modifier ou changer la longueur de votre clé DKIM.

Lorsque votre e-mail est en transit, DNS utilise votre clé publique pour l'authentifier. Par conséquent, si vous changez de clé trop rapidement ou trop fréquemment, DNS peut ne pas être en mesure d'authentifier votre e-mail par DKIM, car l'ancienne clé peut déjà avoir été annulée. Donc, les restrictions suivantes permettent d'éviter cela :

- Vous ne pouvez pas passer à la même longueur de clé que celle qui est déjà configurée.
- Vous ne pouvez pas passer à une longueur de clé différente plus d'une fois au cours d'une période de 24 heures (sauf s'il s'agit de la première rétrogradation à 1024 de cette période).

Lorsque vous utilisez les procédures suivantes pour modifier la longueur de votre clé, si vous dérogez à l'une de ces restrictions, la console renverra une bannière d'erreur indiquant que l'entrée que vous avez fournie n'est pas valide, ainsi que la raison pour laquelle elle ne l'est pas.

Pour modifier les bits de longueur de clé de signature DKIM

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).
3. Dans la liste des identités, choisissez celle pour laquelle vous souhaitez modifier la longueur de la clé de signature DKIM.
4. Sous l'onglet Authentification, dans le conteneur norme DKIM (DomainKeys Identified Mail), choisissez Edit (Modifier).
5. Dans le conteneur Advanced DKIM settings (Paramètres avancés de DKIM), choisissez RSA_2048_BIT ou RSA_1024_BIT dans le champ DKIM signing key length (Longueur de la clé DKIM).
6. Choisissez Enregistrer les modifications.

Fournissez votre propre jeton d'authentification DKIM (BYODKIM) dans Amazon SES

Comme alternative à l'utilisation d'Easy DKIM, vous pouvez configurer l'authentification DKIM en utilisant votre propre paire de clés publique-privée. Ce processus est connu sous le nom de Bring Your Own DKIM (Fournissez votre propre DKIM) (BYODKIM).

Avec BYODKIM, vous pouvez utiliser un registre DNS unique pour configurer l'authentification DKIM pour vos domaines, contrairement à Easy DKIM qui vous oblige à publier trois registres DNS

distincts. En outre, avec BYODKIM, vous pouvez procéder à une rotation des clés DKIM de vos domaines aussi souvent que vous le souhaitez.

Rubriques de cette section :

- Étape 1 : Créer la paire de clés
- Étape 2 : Ajouter la clé publique et le sélecteur à la configuration de domaine de votre fournisseur DNS
- Étape 3 : Configurer et vérifier un domaine pour utiliser BYODKIM

> **Warning**
>
> Si Easy DKIM est actuellement activé et que vous passez à BYODKIM, sachez qu'Amazon SES n'utilisera pas Easy DKIM pour signer vos e-mails pendant la configuration de BYODKIM et que votre statut DKIM est en attente. Entre le moment où vous passez l'appel pour activer BYODKIM (via l'API ou la console) et le moment où SES peut confirmer votre configuration DNS, vos e-mails peuvent être envoyés par SES sans signature DKIM. Par conséquent, il est conseillé d'utiliser une étape intermédiaire pour migrer d'une méthode de signature DKIM à l'autre (par exemple, utiliser un sous-domaine de votre domaine avec Easy DKIM activé, puis la supprimer une fois la vérification BYODKIM passée), ou effectuer cette activité pendant les temps d'arrêt de votre application, le cas échéant.

Étape 1 : Créer la paire de clés

Pour utiliser la fonction Bring Your Own DKIM (Fournissez votre propre DKIM), vous devez d'abord créer une paire de clés RSA.

La clé privée que vous générez doit être au format PKCS #1 ou PKCS #8, utiliser un chiffrement RSA d'au moins1024 bits et jusqu'à 2048 bits, et être encodée à l'aide du codage (PEM) base64. Voir the section called “Longueur de la clé DKIM” pour en savoir plus sur les longueurs des clés de signature DKIM et sur la manière de les modifier.

> **Note**
>
> Vous pouvez utiliser des applications et des outils tiers pour générer des paires de clés RSA tant que la clé privée est générée avec un chiffrement RSA d'au moins 1 024 bits et jusqu'à 2 048 bits, et qu'elle est encodée à l’aide du codage (PEM) base64.

Dans la procédure suivante, l'exemple de code qui utilise la commande `openssl genrsa` intégrée à la plupart des systèmes d'exploitation Linux, macOS ou Unix pour créer la paire de clés utilisera automatiquement le codage (PEM) base64.

Pour créer la paire de clés à partir de la ligne de commande Linux, macOS ou Unix

1. Dans la ligne de commande, entrez la commande suivante pour générer la clé privée remplaçant *nnnn* avec une longueur de bit d'au moins 1024 et jusqu'à 2048 :

   ```
   openssl genrsa -f4 -out private.key nnnn
   ```

2. À partir de la ligne de commande, entrez la commande suivante pour générer la clé publique :

   ```
   openssl rsa -in private.key -outform PEM -pubout -out public.key
   ```

Étape 2 : Ajouter la clé publique et le sélecteur à la configuration de domaine de votre fournisseur DNS

Maintenant que vous avez créé une paire de clés, vous devez ajouter la clé publique à la configuration DNS pour votre domaine en tant qu'registre TXT.

Pour ajouter la clé publique à la configuration DNS pour votre domaine

1. Connectez-vous à la console de gestion de votre fournisseur DNS ou d'hébergement.
2. Ajoutez un nouvel registre texte à la configuration DNS pour votre domaine le registre doit utiliser le format suivant :

Nom	Type	Valeur
selector._domainkey.*example.com*	TXT	p=*yourPublicKey*

   Dans l'exemple précédent, apportez les modifications suivantes :

   - Remplacez *selector* par un nom unique qui identifie la clé.

> **Note**
>
> Un petit nombre de fournisseurs DNS n'autorisent pas l'inclusion de traits de soulignement (_) dans les noms de registre. Cependant, les traits de soulignement dans les noms de registres DKIM sont obligatoires. Si votre fournisseur DNS ne vous permet pas de saisir un caractère de soulignement dans le nom de registre, contactez l'équipe de support client du fournisseur pour obtenir de l'aide.

- Remplacez *`example.com`* par votre domaine.
- Remplacez *`yourPublicKey`* par la clé publique que vous avez créée précédemment et incluez le préfixe p= comme indiqué dans la colonne Value (Valeur) ci-dessus.

> **Note**
>
> Lorsque vous publiez (ajoutez) votre clé publique à votre fournisseur DNS, elle doit être formatée comme suit :
>
> - Vous devez supprimer les première et dernière lignes (respectivement `-----BEGIN PUBLIC KEY-----` et `-----END PUBLIC KEY-----`) de la clé publique générée. En outre, vous devez supprimer les sauts de ligne dans la clé publique générée. La valeur résultante est une chaîne de caractères sans espace ni saut de ligne.
> - Vous devez inclure le préfixe p= comme indiqué dans la colonne Value (Valeur) dans le tableau ci-dessus.

Les différents fournisseurs ont des procédures différentes pour mettre à jour les registres DNS. Le tableau suivant comprend des liens vers de la documentation relative à quelques fournisseurs DNS courants. Cette liste n'est pas exhaustive et n’a pas valeur d’approbation. De même, si votre fournisseur DNS n'est pas répertorié, cela ne signifie pas que vous ne pouvez pas utiliser le domaine avec Amazon SES.

Fournisseur DNS/d'hébergement	Lien vers la documentation
Amazon Route 53	Modification des registres dans le Guide du développeur Amazon Route 53.

Fournisseur DNS/d'hébergement	Lien vers la documentation
GoDaddy	Ajout d'un registre TXT (lien externe)
DreamHost	How do I add custom DNS records? (Comment ajouter des registres DNS personnalisés ?) (lien externe)
Cloudflare	Gestion des registres DNS dans CloudFlare (lien externe)
HostGator	Manage DNS Records with HostGator/eNom (Gérer des registres DNS avec HostGator/eNom) (lien externe)
Namecheap	How do I add TXT/SPF/DKIM/DMARC records for my domain? (Comment ajouter des registres TXT/SPF/DKIM/DMARC pour mon domaine ?) (lien externe)
Names.co.uk	Changing your domains DNS Settings (Modifier vos paramètres DNS de domaine) (lien externe)
Wix	Ajout ou mise à jour des registres TXT dans votre compte Wix (lien externe)

Étape 3 : Configurer et vérifier un domaine pour utiliser BYODKIM

Vous pouvez configurer BYODKIM pour les nouveaux domaines (c'est-à-dire, les domaines que vous n'utilisez pas actuellement pour envoyer des e-mails via Amazon SES) et les domaines existants (c'est-à-dire, les domaines que vous avez déjà configurés pour utiliser avec Amazon SES) en utilisant la console ou AWS CLI. Avant d'effectuer les procédures AWS CLI de cette section, vous devez d'abord installer et configurer AWS CLI. Pour en savoir plus, veuillez consulter le Guide de l'utilisateur AWS Command Line Interface..

Option 1 : Création d'une nouvelle identité de domaine utilisant BYODKIM

Cette section contient les procédures de création d'une identité de domaine utilisant BYODKIM. Une nouvelle identité de domaine est un domaine que vous n'avez pas précédemment configuré pour envoyer des e-mails via Amazon SES.

Si vous souhaitez configurer un domaine existant pour utiliser BYODKIM, effectuez plutôt la procédure décrite dans Option 2 : Configuration d'une identité de domaine existante.

Pour créer une identité à l'aide de BYODKIM depuis la console

- Suivez la procédure dans Création d'une identité de domaine et, lorsque vous arrivez à l'étape 8, suivez les instructions spécifiques à BYODKIM.

Pour créer une identité à l'aide de BYODKIM dans le AWS CLI

Pour configurer un nouveau domaine, utilisez l'opération `CreateEmailIdentity` dans l'API Amazon SES.

1. Dans un éditeur de texte, collez le code suivant :

```
{
    "EmailIdentity":"example.com",
    "DkimSigningAttributes":{
        "DomainSigningPrivateKey":"privateKey",
        "DomainSigningSelector":"selector"
    }
}
```

   Dans l'exemple précédent, apportez les modifications suivantes :

   - Remplacez *`example.com`* par le domaine que vous souhaitez créer.
   - Remplacez *`privateKey`* par votre clé privée.

   > **Note**
   >
   > Vous devez supprimer les première et dernière lignes (respectivement `-----BEGIN PRIVATE KEY-----` et `-----END PRIVATE KEY-----`) de la clé privée générée.

En outre, vous devez supprimer les sauts de ligne dans la clé privée générée. La valeur résultante est une chaîne de caractères sans espace ni saut de ligne.

- Remplacez *selector* par le sélecteur unique que vous avez spécifié lorsque vous avez créé le registre TXT dans la configuration DNS pour votre domaine.

Lorsque vous avez terminé, enregistrez le fichier sous `create-identity.json`.

2. Sur la ligne de commande, entrez la commande suivante :

```
aws sesv2 create-email-identity --cli-input-json file://path/to/create-identity.json
```

Dans la commande précédente, remplacez *path/to/create-identity.json* par le chemin d'accès complet au fichier que vous avez créé à l'étape précédente.

Option 2 : Configuration d'une identité de domaine existante

Cette section contient les procédures de mise à jour d'une identité de domaine existante pour utiliser BYODKIM. Une identité de domaine existante est un domaine que vous avez déjà configuré pour envoyer des e-mails via Amazon SES.

Pour mettre à jour une identité de domaine en utilisant BYODKIM depuis la console

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES sur la page https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).
3. Dans la liste des identités, choisissez une identité dans laquelle le type d'identité est le Domaine.

> **Note**
>
> Si vous devez créer ou vérifier un domaine, veuillez consulter Création d'une identité de domaine.

4. Sous l'onglet Authentification, dans le volet norme DKIM (DomainKeys Identified Mail), choisissez Edit (Modifier).

5. Dans le volet Advanced DKIM settings (Paramètres avancés de DKIM), choisissez Provide DKIM authentication token (BYODKIM) [Fournir un jeton d'authentification DKIM (BYODKIM)] dans la zone Identity type (Type d'identité).
6. Pour Private key (Clé privée), collez la clé privée que vous avez générée précédemment.

   > **Note**
   >
   > Vous devez supprimer les première et dernière lignes (respectivement `-----BEGIN PRIVATE KEY-----` et `-----END PRIVATE KEY-----`) de la clé privée générée. En outre, vous devez supprimer les sauts de ligne dans la clé privée générée. La valeur résultante est une chaîne de caractères sans espace ni saut de ligne.

7. Pour Selector name (Nom du sélecteur, entrez le nom du sélecteur que vous avez spécifié dans les paramètres DNS de votre domaine.
8. Dans DKIM signatures (Signatures DKIM), cochez la case Enabled (Activé).
9. Sélectionnez Save Changes (Enregistrer les modifications).

Pour mettre à jour une identité de domaine à l'aide de BYODKIM AWS CLI

Pour configurer un domaine existant, utilisez l'opération `PutEmailIdentityDkimSigningAttributes` dans l'API Amazon SES.

1. Dans un éditeur de texte, collez le code suivant :

   ```
   {
       "SigningAttributes":{
           "DomainSigningPrivateKey":"privateKey",
           "DomainSigningSelector":"selector"
       },
       "SigningAttributesOrigin":"EXTERNAL"
   }
   ```

   Dans l'exemple précédent, apportez les modifications suivantes :

   - Remplacez *`privateKey`* par votre clé privée.

> **Note**
>
> Vous devez supprimer les première et dernière lignes (respectivement `-----BEGIN PRIVATE KEY-----` et `-----END PRIVATE KEY-----`) de la clé privée générée. En outre, vous devez supprimer les sauts de ligne dans la clé privée générée. La valeur résultante est une chaîne de caractères sans espace ni saut de ligne.

- Remplacez *`selector`* par le sélecteur unique que vous avez spécifié lorsque vous avez créé le registre TXT dans la configuration DNS pour votre domaine.

Lorsque vous avez terminé, enregistrez le fichier sous `update-identity.json`.

2. Sur la ligne de commande, entrez la commande suivante :

```
aws sesv2 put-email-identity-dkim-signing-attributes --email-identity example.com
 --cli-input-json file://path/to/update-identity.json
```

Dans l'exemple précédent, apportez les modifications suivantes :

- Remplacez *`path/to/update-identity.json`* par le chemin d'accès complet au fichier que vous avez créé à l'étape précédente.
- Remplacez *`example.com`* par le domaine que vous souhaitez mettre à jour.

Vérification du statut DKIM pour un domaine qui utilise BYODKIM

Pour vérifier le statut DKIM d'un domaine depuis la console

Après avoir configuré un domaine pour utiliser BYODKIM, vous pouvez utiliser la console SES pour confirmer que DKIM est correctement configuré.

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES sur la page https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).
3. Dans la liste des identités, choisissez l'identité pour laquelle vous souhaitez vérifier le statut DKIM.

4. La propagation des modifications des paramètres DNS peut prendre jusqu'à 72 heures. Dès qu'Amazon SES détecte tous les registres DKIM requis dans les paramètres DNS de votre domaine, le processus de vérification est terminé. Si tout a été correctement configuré, la zone DKIM configuration (Configuration DKIM)de votre domaine affiche Successful (Succès) dans le volet DomainKeys Identified Mail (DKIM) et la zone Identity status (Statut d'identité) affiche Verified (Vérifié) dans le volet Summary (Récapitulatif).

Pour vérifier le statut DKIM d'un domaine à l'aide de la AWS CLI

Après avoir configuré un domaine pour utiliser BYODKIM, vous pouvez utiliser l'opération GetEmailIdentity pour vérifier que DKIM est correctement configuré.

- Sur la ligne de commande, entrez la commande suivante :

  ```
  aws sesv2 get-email-identity --email-identity example.com
  ```

  Dans la commande précédente, remplacez *example.com* par votre domaine.

  Cette commande renvoie un objet JSON qui contient une section semblable à l'exemple suivant.

  ```
  {
      ...
      "DkimAttributes": {
          "SigningAttributesOrigin": "EXTERNAL",
          "SigningEnabled": true,
          "Status": "SUCCESS",
          "Tokens": [ ]
      },
      ...
  }
  ```

  BYODKIM est correctement configuré pour le domaine si toutes les conditions suivantes sont remplies :

  - La valeur de la propriété `SigningAttributesOrigin` est `EXTERNAL`.
  - La valeur de `SigningEnabled` est `true`.
  - La valeur de `Status` est `SUCCESS`.

Gestion d'Easy DKIM et de BYODKIM

Vous pouvez gérer les paramètres DKIM pour vos identités authentifiées à l'aide d'Easy DKIM ou de BYODKIM via la console Amazon SES basée sur le web, ou à l'aide de l'API Amazon SES. Vous pouvez utiliser l'une ou l'autre de ces méthodes pour obtenir les registres DKIM pour une identité, ou pour activer ou désactiver la signature DKIM pour une identité.

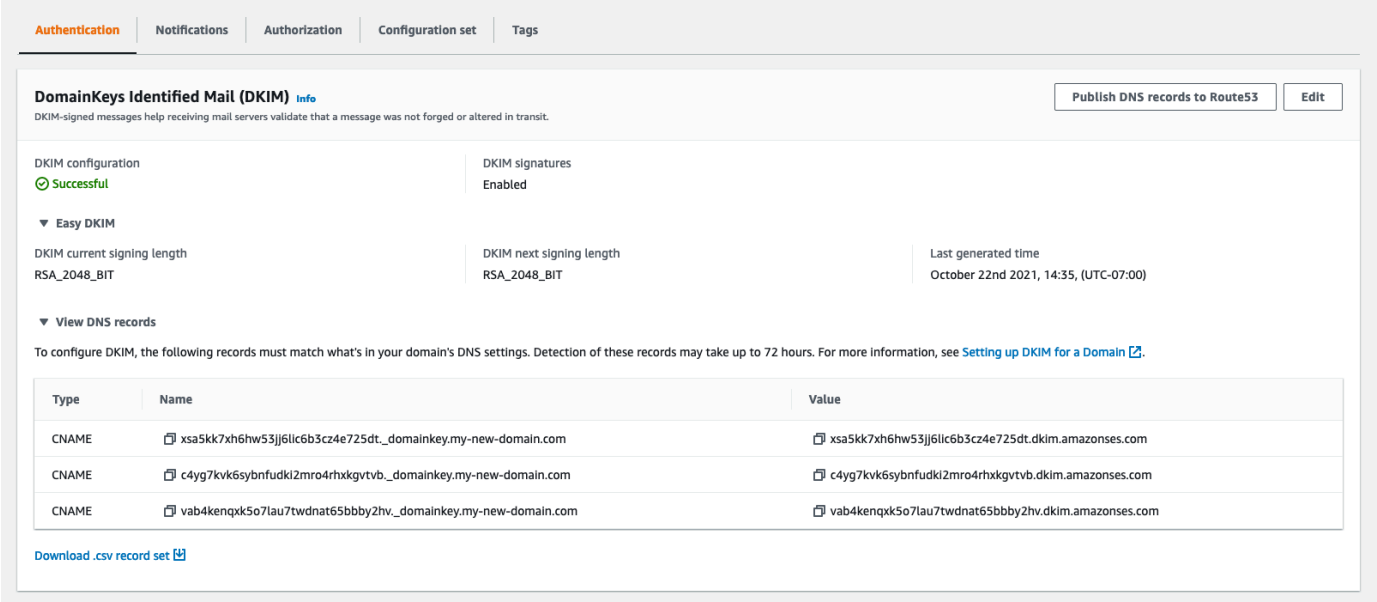
Obtention des registres DKIM pour une identité

Vous pouvez obtenir les registres DKIM pour votre domaine ou votre adresse e-mail à tout moment à l'aide de la console Amazon SES.

Pour obtenir les registres DKIM pour une identité à l'aide de la console

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).
3. Dans la liste des identités, choisissez l'identité pour laquelle vous souhaitez obtenir les registres DKIM.
4. Dans l'onglet Authentification de la page de détails de l'identité, développez View DNS records (Afficher les registres DNS).
5. Copiez soit les trois registres CNAME si vous avez utilisé Easy DKIM, soit le registre TXT si vous avez utilisé BYODKIM, qui apparaissent dans cette section. Sinon, vous pouvez choisir Download Record Set as CSV (Télécharger le jeu de registres au format .csv) pour enregistrer une copie des registres sur votre ordinateur.

   L'image suivante illustre un exemple de la section étendue View DNS records (Afficher les registres DNS) qui présente les registres CNAME associés à Easy DKIM.



Vous pouvez aussi obtenir les registres DKIM d'une identité à l'aide de l'API Amazon SES. Une méthode courante pour interagir avec l'API consiste à utiliser AWS CLI.

Pour obtenir les enregistrements DKIM d'une identité à l'aide du AWS CLI

1. Sur la ligne de commande, entrez la commande suivante :

   ```
   aws ses get-identity-dkim-attributes --identities "example.com"
   ```

   Dans l'exemple précédent, remplacez *example.com* par l'identité pour laquelle vous souhaitez obtenir les registres DKIM. Vous pouvez spécifier une adresse e-mail ou un domaine.

2. La sortie de cette commande contient une section `DkimTokens`, comme illustré dans l'exemple suivant :

   ```
   {
       "DkimAttributes": {
           "example.com": {
               "DkimEnabled": true,
               "DkimVerificationStatus": "Success",
               "DkimTokens": [
                   "hirjd4exampled5477y22yd23ettobi",
                   "v3rnz522czcl46quexamplek3efo5o6x",
                   "y4examplexbhyhnsjcmtvzotfvqjmdqoj"
               ]
   ```

```
        }
    }
}
```

Vous pouvez utiliser les jetons pour créer les registres CNAME que vous ajoutez aux paramètres DNS de votre domaine. Pour créer les registres CNAME, utilisez le modèle suivant :

```
token1._domainkey.example.com CNAME token1.dkim.amazonses.com
token2._domainkey.example.com CNAME token2.dkim.amazonses.com
token3._domainkey.example.com CNAME token3.dkim.amazonses.com
```

Remplacez chaque instance de *token1* par le premier jeton de la liste que vous avez reçue lorsque vous avez exécuté la commande `get-identity-dkim-attributes`, remplacez toutes les instances de *token2* par le deuxième jeton de la liste et remplacez toutes les instances de *token3* par le troisième jeton de la liste.

Par exemple, l'application de ce modèle aux jetons présentés dans l'exemple précédent génère les registres suivants :

```
hirjd4exampled5477y22yd23ettobi._domainkey.example.com CNAME
 hirjd4exampled5477y22yd23ettobi.dkim.amazonses.com
v3rnz522czcl46quexamplek3efo5o6x._domainkey.example.com CNAME
 v3rnz522czcl46quexamplek3efo5o6x.dkim.amazonses.com
y4examplexbhyhnsjcmtvzotfvqjmdqoj._domainkey.example.com CNAME
 y4examplexbhyhnsjcmtvzotfvqjmdqoj.dkim.amazonses.com
```

> **Note**
>
> Si vous avez sélectionné Région AWS Le Cap, Osaka ou Milan, vous devrez utiliser des domaines DKIM spécifiques à la région, comme indiqué dans le tableau des domaines DKIM figurant dans le. Références générales AWS

Désactivation d'Easy DKIM pour une identité

Vous pouvez rapidement désactiver l'authentification DKIM pour une identité à l'aide de la console Amazon SES.

Pour désactiver DKIM pour une identité

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).
3. Dans la liste des identités, choisissez l'identité pour laquelle vous souhaitez désactiver DKIM.
4. Sous l'onglet Authentification, dans le conteneur DomainKeysIdentified Mail (DKIM), choisissez Modifier.
5. Dans Advanced DKIM settings (Paramètres avancés de DKIM), cochez la case Enabled (Activé) dans le champ DKIM signatures (Signatures DKIM).

Vous pouvez également désactiver DKIM pour une identité à l'aide de l'API Amazon SES. Une méthode courante pour interagir avec l'API consiste à utiliser AWS CLI.

Pour désactiver le DKIM pour une identité à l'aide du AWS CLI

- Sur la ligne de commande, entrez la commande suivante :

  ```
  aws ses set-identity-dkim-enabled --identity example.com --no-dkim-enabled
  ```

  Dans l'exemple précédent, remplacez *example.com* par l'identité pour laquelle vous souhaitez désactiver DKIM. Vous pouvez spécifier une adresse e-mail ou un domaine.

Activation d'Easy DKIM pour une identité

Si vous avez déjà désactivé DKIM pour une identité, vous pouvez l'activer à nouveau à l'aide de la console Amazon SES.

Pour activer DKIM pour une identité

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).
3. Dans la liste des identités, choisissez l'identité pour laquelle vous souhaitez activer DKIM.

4. Sous l'onglet Authentification, dans le conteneur DomainKeysIdentified Mail (DKIM), choisissez Modifier.
5. Dans Advanced DKIM settings (Paramètres avancés de DKIM), cochez la case Enabled (Activé) dans la zone DKIM signatures (Signatures DKIM).

Vous pouvez également activer DKIM pour une identité à l'aide de l'API Amazon SES. Une méthode courante pour interagir avec l'API consiste à utiliser AWS CLI.

Pour activer le DKIM pour une identité à l'aide du AWS CLI

- Sur la ligne de commande, entrez la commande suivante :

  ```
  aws ses set-identity-dkim-enabled --identity example.com --dkim-enabled
  ```

  Dans l'exemple précédent, remplacez *example.com* par l'identité pour laquelle vous souhaitez activer DKIM. Vous pouvez spécifier une adresse e-mail ou un domaine.

Remplacement de la signature DKIM héritée sur une identité d'adresse e-mail

Dans cette section, vous découvrirez comment remplacer (désactiver ou activer) les propriétés de signature DKIM héritées du domaine parent sur une identité d'adresse e-mail spécifique déjà vérifiée avec Amazon SES. Cette opération n'est possible que pour les identités d'adresses e-mail qui appartiennent à des domaines dont vous êtes déjà propriétaire, car les paramètres DNS sont configurés au niveau du domaine.

> **Important**
>
> Vous ne pouvez pas désactiver/activer la signature DKIM pour les identités d'adresse e-mail...
>
> - sur des domaines dont vous n'êtes pas le propriétaire. Par exemple, vous ne pouvez pas activer la signature DKIM pour une adresse gmail.com ou hotmail.com,
> - sur des domaines dont vous êtes propriétaire, mais qui n'ont pas encore été vérifiés dans Amazon SES,
> - sur des domaines dont vous êtes propriétaire, mais qui n'ont pas activé la signature DKIM sur le domaine.

Cette section contient les rubriques suivantes :

- Comprendre les propriétés de signature DKIM héritées
- Remplacement de la signature DKIM sur une identité d'adresse e-mail (console)
- Remplacement de la signature DKIM sur une identité d'adresse e-mail (AWS CLI)

Comprendre les propriétés de signature DKIM héritées

Il est important de comprendre d'abord qu'une identité d'adresse e-mail hérite de ses propriétés de signature DKIM de son domaine parent si ce domaine a été configuré avec DKIM, indépendamment du fait que Easy DKIM ou BYODKIM ait été utilisé. Par conséquent, la désactivation ou l'activation de la signature DKIM sur l'identité de l'adresse e-mail remplace les propriétés de signature DKIM du domaine sur la base de ces éléments clés :

- Si vous avez déjà configuré DKIM pour le domaine auquel appartient une adresse e-mail, vous n'avez pas besoin d'activer la signature DKIM pour l'identité de l'adresse e-mail également.
  - Lorsque vous configurez DKIM pour un domaine, Amazon SES authentifie automatiquement chaque e-mail provenant de chaque adresse de ce domaine grâce aux propriétés DKIM héritées du domaine parent.
- Les paramètres DKIM pour une identité d'adresse e-mail spécifique remplacent automatiquement les paramètres du domaine ou du sous-domaine parent (le cas échéant) auquel l'adresse appartient.

Étant donné que les propriétés de signature DKIM de l'identité d'adresse e-mail sont héritées du domaine parent, si vous envisagez de remplacer ces propriétés, vous devez garder à l'esprit les règles hiérarchiques de remplacement, comme expliqué dans le tableau ci-dessous.

La signature DKIM n'est pas activée dans le domaine parent	La signature DKIM est activée dans le domaine parent
Vous ne pouvez pas activer la signature DKIM sur l'identité de l'adresse e-mail.	Vous pouvez désactiver la signature DKIM sur l'identité de l'adresse e-mail.
	Vous pouvez réactiver la signature DKIM sur l'identité de l'adresse e-mail.

Il n'est généralement pas recommandé de désactiver la signature DKIM, car cela risque de ternir la réputation de l'expéditeur et d'augmenter le risque de voir les e-mails que vous envoyez aboutir dans les dossiers de courrier indésirable ou de spam, ou de voir votre domaine usurpé.

Toutefois, il existe la possibilité de remplacer les propriétés de signature DKIM héritées du domaine sur une identité d'adresse e-mail pour tout cas d'utilisation particulier ou décision commerciale externe pour lesquels vous pourriez avoir à désactiver la signature DKIM de façon permanente ou temporaire, ou à la réactiver ultérieurement.

Remplacement de la signature DKIM sur une identité d'adresse e-mail (console)

La procédure suivante de la console SES explique comment remplacer (désactiver ou activer) les propriétés de signature DKIM héritées du domaine parent sur une identité d'adresse e-mail spécifique déjà vérifiée avec Amazon SES.

Pour activer/désactiver la signature DKIM pour une identité d'adresse e-mail à l'aide de la console

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).
3. Dans la liste des identités, choisissez une identité dont l'Identity type (Type d'identité) est Email address (Adresse e-mail) et qui appartient à l'un de vos domaines vérifiés.
4. Sous l'onglet Authentification, dans le conteneur DomainKeys Identified Mail (DKIM), choisissez Modifier.

   > **Note**
   >
   > L'onglet Authentification (Authentification) n'est présent que si l'identité de l'adresse e-mail sélectionnée appartient à un domaine qui a déjà été vérifié par SES. Si vous n'avez pas encore vérifié votre domaine, voir Création d'une identité de domaine.

5. Sous Advanced DKIM settings (Paramètres avancés DKIM), dans le champ DKIM signatures (Signatures DKIM), effacez la case Enabled (Activé) pour désactiver la signature DKIM ou sélectionnez-la pour réactiver la signature DKIM (si elle a été désactivée précédemment).
6. Sélectionnez Enregistrer les modifications.

Remplacement de la signature DKIM sur une identité d'adresse e-mail (AWS CLI)

L'exemple suivant utilise la commande AWS CLI avec une API SES et des paramètres qui remplaceront (désactiveront ou activeront) les propriétés de signature DKIM héritées du domaine parent sur une identité d'adresse e-mail spécifique que vous avez déjà vérifiée auprès de SES.

Pour activer/désactiver la signature DKIM pour une identité d'adresse e-mail à l'aide de la AWS CLI

- En supposant que vous soyez propriétaire du domaine exemple.com et que vous souhaitiez désactiver la signature DKIM pour l'une des adresses e-mail du domaine, dans la ligne de commande, tapez la commande suivante :

```
aws sesv2 put-email-identity-dkim-attributes --email-identity marketing@example.com
 --no-signing-enabled
```

  a. Remplacez *marketing@exemple.com* avec l'identité d'adresse e-mail pour laquelle vous souhaitez désactiver la signature DKIM.

  b. `--no-signing-enabled` désactive la signature DKIM. Pour réactiver la signature DKIM, utilisez `--signing-enabled`.

Signature DKIM manuelle dans Amazon SES

Au lieu d'utiliser Easy DKIM, vous pouvez aussi ajouter manuellement des signatures DKIM à vos messages, puis envoyer ces messages en utilisant Amazon SES. Si vous choisissez de signer manuellement vos messages, vous devez d'abord créer une signature DKIM. Une fois que vous avez créé le message et la signature DKIM, vous pouvez utiliser l'API SendRawEmail pour l'envoyer.

Si vous décidez de signer manuellement vos e-mails, tenez compte des éléments suivants :

- Chaque message que vous envoyez à l'aide d'Amazon SES contient un en-tête DKIM qui fait référence à un domaine de signature d'amazonses.com (c'est-à-dire qu'il contient la chaîne suivante : `d=amazonses.com`). Si vous signez manuellement vos messages, ces derniers doivent inclure deux en-têtes DKIM : un pour votre domaine, et et celui que Amazon SES crée automatiquement pour amazonses.com.
- Amazon SES ne valide pas les signatures DKIM que vous ajoutez manuellement à vos messages. Si la signature DKIM d'un message contient des erreurs, il peut être rejeté par les fournisseurs de messagerie.
- Lorsque vous signez vos messages, vous devez utiliser une longueur de bit d'au moins 1024 bits.

- Ne signez pas les champs suivants : Message-ID, Date, Return-Path (Chemin de retour), Bounces-To.

> **Note**
>
> Si vous utilisez un client de messagerie pour envoyer des e-mails à l'aide de l'interface SMTP Amazon SES, votre client peut exécuter automatiquement la signature DKIM de vos messages. Certains clients peuvent signer certains de ces champs. Consultez la documentation de votre client de messagerie pour savoir quels sont les champs qui sont signés par défaut.

Authentification d'e-mails avec SPF dans Amazon SES

Sender Policy Framework (SPF) est une norme de validation des e-mails conçue pour lutter contre l'usurpation de messagerie. Les propriétaires de domaine utilisent SPF pour indiquer aux fournisseurs de messagerie les serveurs autorisés à envoyer des e-mails à partir de leur domaine. SPF est défini dans RFC 7208.

Les messages que vous envoyez via Amazon SES utilisent automatiquement un sous-domaine `amazonses.com` en tant que domaine MAIL FROM. L'authentification SPF valide avec succès ces messages, parce que le domaine MAIL FROM par défaut correspond à l'application qui a envoyé l'e-mail, dans ce cas SES. Par conséquent, dans SES, le SPF est implicitement configuré pour vous.

Toutefois, si vous ne souhaitez pas utiliser le domaine MAIL FROM par défaut de SES, mais que vous préférez utiliser un sous-domaine d'un domaine que vous possédez, cela est appelé dans SES un domaine MAIL FROM personnalisé. Pour ce faire, vous devez publier votre propre enregistrement SPF pour votre domaine MAIL FROM personnalisé. En outre, SES requiert que vous configuriez un registre MX afin que votre domaine MAIL FROM personnalisé puisse recevoir les notifications de retour à l'expéditeur et de réclamation que les fournisseurs de messagerie vous envoient.

Découvrez comment configurer l'authentification SPF

Des instructions sont données pour configurer votre domaine avec SPF et pour publier les enregistrements MX et SPF (type TXT) dans. the section called “Utilisation d'un domaine MAIL FROM personnalisé”

Utilisation d'un domaine MAIL FROM personnalisé

Lorsqu'un e-mail est envoyé, il possède deux adresses qui indiquent sa source : une adresse d'expédition qui s'affiche pour le destinataire du message et une adresse MAIL FROM qui indique l'origine du message. L'adresse MAIL FROM est parfois appelée enveloppe d'expéditeur, enveloppe from, adresse de retour à l'expéditeur ou adresse de chemin de retour. Les serveurs de messagerie utilisent l'adresse MAIL FROM pour renvoyer des messages de retour à l'expéditeur et d'autres notifications d'erreur. L'adresse MAIL FROM est généralement visible par les destinataires seulement s'ils affichent le code source du message.

Amazon SES définit une valeur de domaine MAIL FROM par défaut pour les messages que vous envoyez, sauf si vous spécifiez votre propre domaine (personnalisé). Cette section présente les avantages de la configuration d'un domaine MAIL FROM personnalisé et inclut les procédures de configuration.

Pourquoi utiliser un domaine MAIL FROM personnalisé ?

Les messages que vous envoyez via Amazon SES utilisent automatiquement un sous-domaine `amazonses.com` en tant que domaine MAIL FROM. L'authentification SPF (Sender Policy Framework) valide avec succès ces messages, parce que le domaine MAIL FROM par défaut correspond à l'application qui a envoyé l'e-mail, dans ce cas SES.

Si vous ne souhaitez pas utiliser le domaine MAIL FROM par défaut de SES et que vous préférez utiliser un sous-domaine d'un domaine qui vous appartient, SES mentionne l'utilisation d'un domaine MAIL FROM personnalisé. Pour ce faire, vous devez publier votre propre enregistrement SPF pour votre domaine MAIL FROM personnalisé. En outre, SES requiert que vous configuriez un registre MX afin que votre domaine puisse recevoir les notifications de retour à l'expéditeur et de réclamation que les fournisseurs de messagerie vous envoient.

En utilisant un domaine MAIL FROM personnalisé, vous pouvez utiliser SPF, DKIM ou les deux pour obtenir la validation DMARC (Domain-based Message Authentication, Reporting and Conformance). La spécification DMARC permet au domaine d'un expéditeur d'indiquer que les e-mails envoyés depuis le domaine sont protégés par un ou plusieurs systèmes d'authentification. Il existe deux façons de passer la validation DMARC : avec the section called “Conformité à DMARC via SPF” ou the section called “Conformité à DMARC via DKIM”.

Choix d'un domaine MAIL FROM personnalisé

Dans ce qui suit, le terme domaine MAIL FROM fait toujours référence à un sous-domaine d'un domaine que vous possédez. Ce sous-domaine que vous utilisez pour votre domaine MAIL FROM personnalisé ne doit pas être utilisé pour autre chose et répond aux exigences suivantes :

- Le domaine MAIL FROM doit être un sous-domaine du domaine parent d'une identité vérifiée (adresse e-mail ou domaine).
- Le domaine MAIL FROM ne doit pas être un sous-domaine que vous utilisez également pour envoyer des e-mails.
- Le domaine MAIL FROM ne doit pas être un sous-domaine que vous utilisez pour recevoir des e-mails.

Utilisation de SPF avec votre domaine MAIL FROM personnalisé

Sender Policy Framework (SPF) est une norme de validation des e-mails conçue pour lutter contre l'usurpation de messagerie. Vous pouvez configurer votre domaine MAIL FROM personnalisé avec SPF pour indiquer aux fournisseurs de messagerie quels serveurs sont autorisés à envoyer des e-mails à partir de votre domaine MAIL FROM personnalisé. SPF est défini dans RFC 7208.

Pour configurer SPF, vous publiez un registre TXT sur la configuration DNS de votre domaine MAIL FROM personnalisé. Cet registre contient une liste des serveurs que vous autorisez à envoyer des e-mails à partir de votre domaine MAIL FROM personnalisé. Lorsqu'un fournisseur de messagerie reçoit un message de votre domaine MAIL FROM personnalisé, il vérifie les registres DNS de votre domaine pour s'assurer que l'e-mail a été envoyé à partir d'un serveur autorisé.

Si vous souhaitez utiliser cet enregistrement SPF pour vous conformer à la norme DMARC, le domaine indiqué dans l'adresse de l'expéditeur doit correspondre au domaine MAIL FROM. veuillez consulter the section called “Conformité à DMARC via SPF”.

La section suivante, the section called “Configuration de votre domaine MAIL FROM personnalisé”, explique comment configurer SPF pour votre domaine MAIL FROM personnalisé.

Configuration de votre domaine MAIL FROM personnalisé

Le processus de configuration d'un domaine MAIL FROM personnalisé nécessite que vous ajoutiez des registres à la configuration DNS du domaine. SES vous demande de publier un enregistrement MX afin que votre domaine puisse recevoir les notifications de rebond et de réclamation que les

fournisseurs de messagerie vous envoient. Vous devez également publier un registre SPF (type TXT) afin de prouver qu'Amazon SES est autorisé à envoyer des e-mails à partir de votre domaine.

Vous pouvez configurer un domaine MAIL FROM personnalisé pour un domaine entier ou un sous-domaine, ainsi que pour des adresses e-mail individuelles. Les procédures suivantes montrent comment utiliser la console Amazon SES pour configurer un domaine MAIL FROM personnalisé. Vous pouvez également configurer un domaine MAIL FROM personnalisé à l'aide de l'opération SetIdentityMailFromDomain API.

Configuration d'un domaine MAIL FROM personnalisé pour un domaine vérifié

Ces procédures vous montrent comment configurer un domaine MAIL FROM personnalisé pour un domaine entier ou un sous-domaine afin que tous les messages envoyés depuis les adresses de ce domaine utilisent ce domaine MAIL FROM personnalisé.

Pour configurer un domaine vérifié afin d'utiliser un domaine MAIL FROM personnalisé spécifié

1. Ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation de gauche, sous Configuration, sélectionnez Identités.
3. Dans la liste des identités, choisissez l'identité que vous souhaitez configurer pour laquelle Identity type (Type d'identité) est Domain (Domaine) et Status (État) est Verified (Vérifié).
    - Si l'icône Status (État) est Unverified (Non vérifié), complétez les procédures de la section Vérification d’une identité de domaine DKIM auprès de votre fournisseur DNS pour vérifier le domaine de l'adresse e-mail.
4. Au bas de l'écran dans le panneau Custom MAIL FROM domain (Domaine MAIL FROM personnalisé), choisissez Edit (Modifier).
5. Dans le panneau General details (Informations générales), procédez de la façon suivante :
    a. Cochez la case Use a custom MAIL FROM domain (Utiliser un domaine MAIL FROM personnalisé).
    b. Pour MAIL FROM domain (Domaine MAIL FROM), entrez le sous-domaine que vous souhaitez utiliser en tant que domaine MAIL FROM.
    c. Pour Behavior on MX failure (Comportement en cas d'échec MX), choisissez l'une des options suivantes :
        - Use default MAIL FROM domain (Utiliser le domaine MAIL FROM par défaut) – Si l'enregistrement MX du domaine MAIL FROM personnalisé n'est pas configuré

correctement, Amazon SES utilise un sous-domaine de `amazonses.com`. Le sous-domaine varie en fonction du domaine dans Région AWS lequel vous utilisez Amazon SES.

- Reject message (Message rejeté) – Si le registre MX du domaine MAIL FROM personnalisé n'est pas configuré correctement, Amazon SES retourne une erreur `MailFromDomainNotVerified`. Les e-mails que vous essayez d'envoyer à partir de ce domaine sont automatiquement rejetés.

d. Choisissez Save changes (Enregistrer les modifications) ; vous reviendrez à l'écran précédent.

6. Publiez les enregistrements MX et SPF (type TXT) sur le serveur DNS du domaine MAIL FROM personnalisé.

   Dans le volet Custom MAIL FROM domain (Domaine MAIL FROM personnalisé), le tableau Publish DNS records (Publier les enregistrements DNS) affiche maintenant les enregistrements MX et SPF (type TXT) que vous devez publier (ajouter) à la configuration DNS de votre domaine. Ces registres utilisent les formats indiqués dans le tableau suivant.

Nom	Type	Valeur
sous-domaine .*domaine*.*com*	MX	10 feedback-smtp.*region*.amazonses.com
sous-domaine .*domaine*.*com*	TXT	"v=spf1 include:amazonses.com ~all"

   Dans les enregistrements précédents,

   - *subdomain*.*domain*.*com* sera renseigné avec votre sous-domaine MAIL FROM ;
   - *la région* sera renseignée avec le nom de l' Région AWS endroit où vous souhaitez vérifier le domaine MAIL FROM (tel que `us-west-2us-east-1`, o`ueu-west-1`, etc.)
   - Le nombre 10 en regard de la valeur MX est l'ordre de préférence du serveur de messagerie et devra être entré dans un champ de valeur distinct tel que spécifié par l'interface graphique de votre fournisseur DNS ;
   - La valeur d’enregistrement TXT SPF doit inclure des guillemets.

À partir du tableau Publish DNS records (Publier les enregistrements DNS), copiez les enregistrements MX et SPF (type TXT) en choisissant l'icône de copie en regard de chaque valeur et collez-les dans les champs correspondants de l'interface graphique de votre fournisseur DNS. Sinon, vous pouvez choisir Download Record Set as CSV (Télécharger le jeu de registres au format .csv) pour enregistrer une copie des registres sur votre ordinateur.

> **Important**
>
> Pour configurer correctement un domaine MAIL FROM personnalisé avec Amazon SES, vous devez publier un seul registre MX sur le serveur DNS de votre domaine MAIL FROM. Si le domaine MAIL FROM a plusieurs registres MX, la configuration MAIL FROM personnalisée avec Amazon SES échoue.

Si Route 53 fournit le service DNS pour votre domaine MAIL FROM et que vous êtes connecté au même compte que AWS Management Console celui que vous utilisez pour Route 53, choisissez Publier les enregistrements à l'aide de Route 53. Les registres DNS sont automatiquement appliqués à la configuration DNS de votre domaine.

Si vous utilisez un autre fournisseur DNS, vous devez publier manuellement les registres DNS sur le serveur DNS du domaine MAIL FROM. La procédure d'ajout de registres DNS au serveur DNS de votre domaine varie en fonction de votre service d'hébergement web ou de votre fournisseur DNS.

Les procédures de publication des registres DNS de votre domaine varient en fonction du fournisseur DNS que vous utilisez. Le tableau suivant comprend des liens vers de la documentation relative à quelques fournisseurs DNS courants. Cette liste n'est pas exhaustive et n’a pas valeur d'approbation. De même, si votre fournisseur DNS n'est pas répertorié, cela ne signifie pas qu'il ne prend pas en charge la configuration du domaine MAIL FROM.

Nom du fournisseur DNS/d'hébergement	Lien vers la documentation
GoDaddy	• MX : Ajout d'un registre MX (lien externe) • TXT : Ajout d'un registre TXT (lien externe)

Nom du fournisseur DNS/d'hébergement	Lien vers la documentation
DreamHost	• MX : Comment puis-je modifier mes registres MX ? (lien externe) • TXT : Comment puis-je ajouter des registres DNS personnalisés ? (lien externe)
Cloudflare	• MX : Comment puis-je ajouter ou modifier des e-mails ou des registres MX ? (lien externe) • TXT : Gestion des registres DNS dans CloudFlare (lien externe)
HostGator	• MX : Configuration des enregistrements MX (lien externe) • TXT : Gérer les enregistrements DNS avec HostGator /eNom (lien externe)
Namecheap	• MX : Comment puis-je configurer des registres MX requis pour le service de messagerie ? (lien externe) • TXT : Comment puis-je ajouter des registres TXT/SPF/DKIM/DMARC pour mon domaine ? (lien externe)
Names.co.uk	• MX : Modification des paramètres DNS de votre domaine (lien externe) • TXT : Modification de vos paramètres DNS de domaine (lien externe)
Wix	• MX : Ajout ou mise à jour des registres MX de votre compte Wix (lien externe) • TXT : Ajout ou mise à jour des registres TXT dans votre compte Wix (lien externe)

Quand Amazon SES détecte que les registres sont en place, vous recevez un e-mail vous informant que votre domaine MAIL FROM personnalisé a été configuré avec succès. En fonction de votre fournisseur DNS, il peut y avoir un délai de 72 heures avant qu'Amazon SES ne détecte le registre MX.

Configuration d'un domaine MAIL FROM personnalisé pour une adresse e-mail vérifiée

Vous pouvez également configurer un domaine MAIL FROM personnalisé pour une adresse e-mail spécifique. Pour configurer un domaine MAIL FROM personnalisé pour une adresse e-mail, vous devez modifier les registres DNS pour le domaine auquel l'adresse e-mail est associée.

> **Note**
>
> Vous ne pouvez pas configurer un domaine MAIL FROM personnalisé pour les adresses d'un domaine qui ne vous appartient pas (par exemple, vous ne pouvez pas créer un domaine MAIL FROM personnalisé pour une adresse sur le domaine `gmail.com`, car vous ne pouvez pas ajouter les registres DNS nécessaires au domaine).

Pour configurer une adresse e-mail vérifiée afin qu'elle utilise un domaine MAIL FROM spécifié

1. Ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation de gauche, sous Configuration, sélectionnez Identités.
3. Dans la liste des identités, choisissez l'identité que vous souhaitez configurer pour laquelle Identity type (Type d'identité) est Email address (Adresse e-mail) et Status (État) est Verified (Vérifié).
   - Si l'icône Status (État) est Unverified (Non vérifié), complétez les procédures de la section Vérification d'une identité d'adresse e-mail pour vérifier le domaine de l'adresse e-mail.
4. Sous l'onglet MAIL FROM Domain (Domaine MAIL FROM), choisissez Edit (Modifier) dans le panneau Custom MAIL FROM domain (Domaine MAIL FROM personnalisé).
5. Dans le panneau General details (Informations générales), procédez de la façon suivante :
   a. Cochez la case Use a custom MAIL FROM domain (Utiliser un domaine MAIL FROM personnalisé).

b. Pour MAIL FROM domain (Domaine MAIL FROM), entrez le sous-domaine que vous souhaitez utiliser en tant que domaine MAIL FROM.

c. Pour Behavior on MX failure (Comportement en cas d'échec MX), choisissez l'une des options suivantes :

- Use default MAIL FROM domain (Utiliser le domaine MAIL FROM par défaut) – Si l'enregistrement MX du domaine MAIL FROM personnalisé n'est pas configuré correctement, Amazon SES utilise un sous-domaine de `amazonses.com`. Le sous-domaine varie en fonction du domaine dans Région AWS lequel vous utilisez Amazon SES.
- Reject message (Message rejeté) – Si le registre MX du domaine MAIL FROM personnalisé n'est pas configuré correctement, Amazon SES retourne une erreur `MailFromDomainNotVerified`. Les e-mails que vous essayez d'envoyer à partir de cette adresse sont automatiquement rejetés.

d. Choisissez Save changes (Enregistrer les modifications) ; vous reviendrez à l'écran précédent.

6. Publiez les enregistrements MX et SPF (type TXT) sur le serveur DNS du domaine MAIL FROM personnalisé.

   Dans le volet Custom MAIL FROM domain (Domaine MAIL FROM personnalisé), le tableau Publish DNS records (Publier les enregistrements DNS) affiche maintenant les enregistrements MX et SPF (type TXT) que vous devez publier (ajouter) à la configuration DNS de votre domaine. Ces registres utilisent les formats indiqués dans le tableau suivant.

Nom	Type	Valeur
sous-domaine.*domaine*.*com*	MX	10 feedback-smtp.*region*.amazonses.com
sous-domaine.*domaine*.*com*	TXT	"v=spf1 include:amazonses.com ~all"

   Dans les enregistrements précédents,

- *subdomain*.*domain*.*com* sera renseigné avec votre sous-domaine MAIL FROM ;

- *la région* sera renseignée avec le nom de l' Région AWS endroit où vous souhaitez vérifier le domaine MAIL FROM (tel que `us-west-2us-east-1`, o`ueu-west-1`, etc.)
- Le nombre 10 en regard de la valeur MX est l'ordre de préférence du serveur de messagerie et devra être entré dans un champ de valeur distinct tel que spécifié par l'interface graphique de votre fournisseur DNS ;
- La valeur d'enregistrement TXT SPF doit inclure des guillemets.

À partir du tableau Publish DNS records (Publier les enregistrements DNS), copiez les enregistrements MX et SPF (type TXT) en choisissant l'icône de copie en regard de chaque valeur et collez-les dans les champs correspondants de l'interface graphique de votre fournisseur DNS. Sinon, vous pouvez choisir Download Record Set as CSV (Télécharger le jeu de registres au format .csv) pour enregistrer une copie des registres sur votre ordinateur.

> **Important**
>
> Pour configurer correctement un domaine MAIL FROM personnalisé avec Amazon SES, vous devez publier un seul registre MX sur le serveur DNS de votre domaine MAIL FROM. Si le domaine MAIL FROM a plusieurs registres MX, la configuration MAIL FROM personnalisée avec Amazon SES échoue.

Si Route 53 fournit le service DNS pour votre domaine MAIL FROM et que vous êtes connecté au même compte que AWS Management Console celui que vous utilisez pour Route 53, choisissez Publier les enregistrements à l'aide de Route 53. Les registres DNS sont automatiquement appliqués à la configuration DNS de votre domaine.

Si vous utilisez un autre fournisseur DNS, vous devez publier manuellement les registres DNS sur le serveur DNS du domaine MAIL FROM. La procédure d'ajout de registres DNS au serveur DNS de votre domaine varie en fonction de votre service d'hébergement web ou de votre fournisseur DNS.

Les procédures de publication des registres DNS de votre domaine varient en fonction du fournisseur DNS que vous utilisez. Le tableau suivant comprend des liens vers de la documentation relative à quelques fournisseurs DNS courants. Cette liste n'est pas exhaustive et n'a pas valeur d'approbation. De même, si votre fournisseur DNS n'est pas répertorié, cela ne signifie pas qu'il ne prend pas en charge la configuration du domaine MAIL FROM.

Nom du fournisseur DNS/d'hébergement	Lien vers la documentation
GoDaddy	• MX : Ajout d'un registre MX (lien externe) • TXT : Ajout d'un registre TXT (lien externe)
DreamHost	• MX : Comment puis-je modifier mes registres MX ? (lien externe) • TXT : Comment puis-je ajouter des registres DNS personnalisés ? (lien externe)
Cloudflare	• MX : Comment puis-je ajouter ou modifier des e-mails ou des registres MX ? (lien externe) • TXT : Gestion des registres DNS dans CloudFlare (lien externe)
HostGator	• MX : Modification des registres MX - Windows (lien externe) • TXT : Gérer les enregistrements DNS avec HostGator /eNom (lien externe)
Namecheap	• MX : Comment puis-je configurer des registres MX requis pour le service de messagerie ? (lien externe) • TXT : Comment puis-je ajouter des registres TXT/SPF/DKIM/DMARC pour mon domaine ? (lien externe)
Names.co.uk	• MX : Modification des paramètres DNS de votre domaine (lien externe) • TXT : Modification de vos paramètres DNS de domaine (lien externe)

Nom du fournisseur DNS/d'hébergement	Lien vers la documentation
Wix	• MX : Ajout ou mise à jour des registres MX de votre compte Wix (lien externe) • TXT : Ajout ou mise à jour des registres TXT dans votre compte Wix (lien externe)

Quand Amazon SES détecte que les registres sont en place, vous recevez un e-mail vous informant que votre domaine MAIL FROM personnalisé a été configuré avec succès. En fonction de votre fournisseur DNS, il peut y avoir un délai de 72 heures avant qu'Amazon SES ne détecte le registre MX.

États de configuration du domaine MAIL FROM personnalisé avec Amazon SES

Une fois que vous avez configuré une identité pour qu'elle utilise un domaine MAIL FROM personnalisé, l'état de la configuration est « pending » (« en attente ») tandis qu'Amazon SES tente de détecter le registre MX requis dans vos paramètres DNS. L'état est alors modifié selon qu'Amazon SES détecte le registre MX. Le tableau suivant décrit le comportement d'envoi d'e-mails, ainsi que les actions Amazon SES associées à chaque état. Chaque fois que l'état change, Amazon SES envoie une notification à l'adresse e-mail associée à votre Compte AWS.

État	Comportement d'envoi d'e-mails	Actions Amazon SES
En attente	Utilise le paramètre de rechange MAIL FROM personnalisé	Amazon SES tente de détecter le registre MX requis pendant 72 heures. En cas d'échec, l'état devient « Failed ».
Réussite	Utilise le domaine MAIL FROM personnalisé	Amazon SES vérifie continuellement que le

État	Comportement d'envoi d'e-mails	Actions Amazon SES
		registre MX requis est en place.
Temporary Failure	Utilise le paramètre de rechange MAIL FROM personnalisé	Amazon SES tente de détecter le registre MX requis pendant 72 heures. En cas d'échec, l'état devient « Failed » ; en cas de succès, l'état devient « Success ».
Échec	Utilise le paramètre de rechange MAIL FROM personnalisé	Amazon SES ne tente plus de détecter le registre MX requis. Pour utiliser un domaine MAIL FROM personnalisé, vous devez redémarrer le processus de configuration dans Configuration de votre domaine MAIL FROM personnalisé.

Mise en conformité au protocole d'authentification DMARC dans Amazon SES

L'authentification, le reporting et la conformité des messages basés sur le domaine (DMARC) est un protocole d'authentification des e-mails qui utilise le Sender Policy Framework (SPF) et le courrier DomainKeys identifié (DKIM) pour détecter l'usurpation d'e-mail et le phishing. Pour être conformes au DMARC, les messages doivent être authentifiés par le biais du SPF ou du DKIM, mais idéalement, lorsque les deux sont utilisés avec le DMARC, vous garantissez le plus haut niveau de protection possible pour l'envoi de vos e-mails.

Passons brièvement en revue ce que fait chacun d'eux et comment le DMARC les lie tous ensemble :

- SPF — Identifie les serveurs de messagerie autorisés à envoyer des e-mails au nom de votre domaine MAIL FROM personnalisé via un enregistrement DNS TXT utilisé par le DNS. Les systèmes de messagerie des destinataires se réfèrent à l'enregistrement TXT SPF pour déterminer si un message provenant de votre domaine personnalisé provient d'un serveur de messagerie autorisé. Fondamentalement, le SPF est conçu pour aider à prévenir l'usurpation d'identité, mais il existe des techniques d'usurpation auxquelles le SPF est susceptible d'être utilisé dans la pratique. C'est pourquoi vous devez également utiliser le DKIM en même temps que le DMARC.
- DKIM — Ajoute une signature numérique à vos messages sortants dans l'en-tête de l'e-mail. Les systèmes de réception de courrier électronique peuvent utiliser cette signature numérique pour vérifier si le courrier entrant est signé par une clé appartenant au domaine. Toutefois, lorsqu'un système de courrier électronique de réception transmet un message, l'enveloppe du message est modifiée de manière à invalider l'authentification SPF. Comme la signature numérique est conservée dans le message électronique parce qu'elle fait partie de l'en-tête du message, DKIM fonctionne même lorsqu'un message a été transféré entre les serveurs de messagerie (tant que le contenu du message n'a pas été modifié).
- DMARC — Garantit l'alignement du domaine avec au moins l'un des formats SPF et DKIM. L'utilisation du SPF et du DKIM à elle seule ne garantit pas que l'adresse d'expéditeur est authentifiée (il s'agit de l'adresse e-mail que votre destinataire voit dans son client de messagerie). SPF vérifie uniquement le domaine spécifié dans l'adresse MAIL FROM (non vu par votre destinataire). DKIM vérifie uniquement le domaine spécifié dans la signature DKIM (également invisible pour votre destinataire). Le DMARC résout ces deux problèmes en exigeant que l'alignement des domaines soit correct sur le SPF ou sur le DKIM :
  - Pour que le SPF passe l'alignement DMARC, le domaine de l'adresse d'origine doit correspondre au domaine de l'adresse MAIL FROM (également appelé chemin de retour et adresse d'enveloppe d'origine). Cela est rarement possible avec le courrier transféré parce qu'il est supprimé ou lorsque le courrier est envoyé par le biais de fournisseurs de messagerie groupés

tiers, car le chemin de retour (MAIL FROM) est utilisé pour les rebonds et les plaintes que le fournisseur (SES) suit à l'aide d'une adresse qu'il possède.

- Pour que le DKIM passe l'alignement DMARC, le domaine spécifié dans la signature DKIM doit correspondre au domaine indiqué dans l'adresse d'origine. Si vous utilisez des expéditeurs ou des services tiers qui envoient du courrier en votre nom, vous pouvez le faire en vous assurant que l'expéditeur tiers est correctement configuré pour la signature DKIM et que vous avez ajouté les enregistrements DNS appropriés dans votre domaine. Les serveurs de messagerie de réception seront alors en mesure de vérifier le courrier électronique qui leur est envoyé par votre tiers comme s'il s'agissait d'un e-mail envoyé par une personne autorisée à utiliser une adresse du domaine.

Tout mettre en place avec le DMARC

Les contrôles d'alignement DMARC dont nous avons parlé ci-dessus montrent comment SPF, DKIM et DMARC fonctionnent tous ensemble pour renforcer la confiance dans votre domaine et la livraison de vos e-mails dans les boîtes de réception. Pour ce faire, le DMARC s'assure que l'adresse de provenance, vue par le destinataire, est authentifiée par le SPF ou le DKIM :

- Un message passe le DMARC si l'un ou les deux contrôles SPF ou DKIM décrits sont réussis.
- Un message échoue au DMARC si les deux contrôles SPF ou DKIM décrits échouent.

Par conséquent, le SPF et le DKIM sont tous deux nécessaires pour que le DMARC ait les meilleures chances d'authentifier votre courrier électronique envoyé, et en utilisant les trois, vous contribuerez à garantir un domaine d'envoi entièrement protégé.

Le DMARC vous permet également d'indiquer aux serveurs de messagerie comment traiter les e-mails lorsqu'ils échouent à l'authentification DMARC grâce à des politiques que vous définissez. Cela sera expliqué dans la section suivantethe section called “Configuration de la stratégie DMARC sur votre domaine”, qui contient des informations sur la façon de configurer vos domaines SES afin que les e-mails que vous envoyez soient conformes au protocole d'authentification DMARC via SPF et DKIM.

Configuration de la stratégie DMARC sur votre domaine

Pour configurer DMARC, vous devez modifier les paramètres DNS de votre domaine. Les paramètres DNS de votre domaine doivent inclure un registre TXT qui spécifie les paramètres DMARC du domaine. Les procédures d'ajout de registres TXT à votre configuration DNS dépendent du

fournisseur DNS ou d'hébergement que vous utilisez. Si vous utilisez Route 53, veuillez consulter Utilisation des registres dans le Guide du développeur Amazon Route 53. Si vous utilisez un autre fournisseur, consultez la documentation de configuration DNS de celui-ci.

Le nom de le registre TXT que vous créez doit être `_dmarc.`*`example.com`*, où *`example.com`* est votre domaine. La valeur de le registre TXT contient la stratégie DMARC qui s'applique à votre domaine. Voici un exemple de registre TXT qui contient une stratégie DMARC :

Nom	Type	Valeur
`_dmarc.example.com`	`TXT`	`"v=DMARC1;p=quarantine;rua=mailto:my_dmarc_report@example.com"`

Dans l'exemple de politique DMARC précédent, cette politique indique aux fournisseurs de messagerie de faire ce qui suit :

- Pour tous les messages dont l'authentification échoue, envoyez-les dans le dossier Spam comme indiqué par le paramètre de politique,`p=quarantine`. Les autres options incluent le fait de ne rien faire en utilisant`p=none`, ou de rejeter purement et simplement le message en utilisant`p=reject`.
  - La section suivante explique comment et quand utiliser ces trois paramètres de politique. Si vous utilisez le mauvais paramètre au mauvais moment, votre e-mail ne sera pas livré, voirthe section called “Mise en œuvre du DMARC”.
- Envoyez des rapports sur tous les e-mails dont l'authentification a échoué dans un résumé (c'est-à-dire un rapport qui agrège les données pour une certaine période, plutôt que d'envoyer des rapports individuels pour chaque événement) comme spécifié par le paramètre de rapport `rua=mailto:my_dmarc_report@example.com` (rua signifie Reporting URI for Aggregate reports). En règle générale, les fournisseurs de messagerie envoient ces rapports consolidés une fois par jour, même si ces stratégies diffèrent d'un fournisseur à l'autre.

Pour en savoir plus sur la configuration DMARC pour votre domaine, consultez sa présentation sur le site web DMARC.

Pour les spécifications complètes du système DMARC, voir le projet DMARC de l'Internet Engineering Task Force (IETF).

Bonnes pratiques pour la mise en œuvre du DMARC

Il est préférable de mettre en œuvre l'application de votre politique DMARC de manière progressive et progressive afin de ne pas interrompre le reste de votre flux de messagerie. Créez et mettez en œuvre un plan de déploiement qui suit ces étapes. Effectuez chacune de ces étapes d'abord avec chacun de vos sous-domaines, puis avec le domaine de premier niveau de votre organisation avant de passer à l'étape suivante.

1. Surveillez l'impact de la mise en œuvre du DMARC (p=none).
   - Commencez par un simple enregistrement en mode surveillance pour un sous-domaine ou un domaine qui demande aux organisations de réception de courrier de vous envoyer des statistiques sur les messages qu'elles voient en utilisant ce domaine. Un enregistrement en mode surveillance est un enregistrement TXT DMARC dont la politique est définie sur aucune. `p=none`
   - Les rapports générés par le biais du DMARC indiqueront les numéros et les sources des messages qui passent ces contrôles, par rapport à ceux qui ne le sont pas. Vous pouvez facilement voir quelle part de votre trafic légitime est ou n'est pas couverte par eux. Vous verrez des signes de transfert, car les messages transférés échoueront au SPF et au DKIM si le contenu est modifié. Vous commencerez également à voir combien de messages frauduleux sont envoyés et d'où ils proviennent.
   - Les objectifs de cette étape sont de savoir quels e-mails seront affectés lorsque vous mettrez en œuvre l'une des deux étapes suivantes, et de faire en sorte que les expéditeurs tiers ou autorisés alignent leurs politiques SPF ou DKIM.
   - Idéal pour les domaines existants.
2. Demandez aux systèmes de messagerie externes de mettre en quarantaine les messages qui ne répondent pas au DMARC (p=quarantine).
   - Lorsque vous pensez que la totalité ou la majeure partie de votre trafic légitime est envoyée par un domaine correspondant au SPF ou au DKIM, et que vous comprenez l'impact de la mise en œuvre du DMARC, vous pouvez mettre en œuvre une politique de quarantaine. Une politique de quarantaine est un enregistrement TXT DMARC dont la politique est définie pour être mise en quarantainep=`quarantine`. Ce faisant, vous demandez aux destinataires du DMARC de placer les messages de votre domaine qui ne répondent pas au DMARC dans l'équivalent local d'un dossier de spam plutôt que dans les boîtes de réception de vos clients.
   - Idéal pour les domaines de transition qui ont analysé les rapports DMARC au cours de l'étape 1.
3. Demandez aux systèmes de messagerie externes de ne pas accepter les messages qui ne répondent pas au DMARC (p=reject).

- La mise en œuvre d'une politique de rejet est généralement la dernière étape. Une politique de rejet est un enregistrement TXT DMARC dont la politique est définie pour rejeterp=`reject`. Ce faisant, vous demandez aux destinataires du DMARC de ne pas accepter les messages qui échouent aux vérifications DMARC. Cela signifie qu'ils ne seront même pas placés en quarantaine dans un dossier de spam ou de courrier indésirable, mais qu'ils seront purement et simplement rejetés.
- Lorsque vous utilisez une politique de rejet, vous saurez exactement quels messages ne sont pas conformes à la politique DMARC, car le rejet entraînera un rebond SMTP. Dans le cas de la quarantaine, les données agrégées fournissent des informations sur les pourcentages d'e-mails réussis ou échoués aux contrôles SPF, DKIM et DMARC.
- Idéal pour les nouveaux domaines ou les domaines existants qui ont suivi les deux étapes précédentes.

Conformité à DMARC via SPF

Pour qu'un e-mail soit conforme à DMARC basé sur SPF, les deux conditions suivantes doivent être remplies :

- Le message doit passer une vérification SPF basée sur un enregistrement SPF (type TXT) valide que vous devez publier dans la configuration DNS de votre domaine MAIL FROM personnalisé.
- Le domaine indiqué dans l'adresse From de l'en-tête de l'e-mail doit correspondre au domaine, ou à un sous-domaine de, spécifié dans l'adresse MAIL FROM. Pour que le SPF soit aligné sur SES, la politique DMARC du domaine ne doit pas spécifier de politique SPF stricte (aspf=s).

Pour se conformer à ces exigences, complétez les étapes suivantes :

- Configurez un domaine MAIL FROM personnalisé en exécutant les procédures de the section called “Utilisation d'un domaine MAIL FROM personnalisé”.
- Assurez-vous que votre domaine d'envoi utilise une stratégie souple pour SPF. Si vous n'avez pas modifié l'alignement des politiques de votre domaine, celui-ci utilise une politique souple par défaut, comme le fait SES.

> **Note**
>
> Vous pouvez déterminer l'alignement DMARC de votre domaine pour SPF en tapant la commande suivante sur la ligne de commande et en remplaçant *example.com* par votre domaine :
>
> ```
> dig -type=TXT _dmarc.example.com
> ```
>
> Dans le résultat de la commande, sous Non-authoritative answer, recherchez un registre qui commence par `v=DMARC1`. Si cet registre inclut la chaîne `aspf=r`, ou si la chaîne `aspf` n'est pas du tout présente, votre domaine utilise l'alignement souple pour SPF. Si le registre inclut la chaîne `aspf=s`, votre domaine utilise l'alignement strict pour SPF. Votre administrateur système doit supprimer cette balise de le registre TXT DMARC dans la configuration DNS de votre domaine.
> Vous pouvez également utiliser un outil de recherche DMARC basé sur le Web, tel que le DMARC Inspector du site Web de dmarcian ou l'outil de vérification DMARC du site MxToolBox Web, pour déterminer l'alignement des politiques de votre domaine en matière de SPF.

Conformité à DMARC via DKIM

Pour qu'un e-mail soit conforme à DMARC basé sur DKIM, les deux conditions suivantes doivent être remplies :

- Le message doit comporter une signature DKIM valide et réussir le contrôle DKIM.
- Le domaine spécifié dans la signature DKIM doit être aligné (correspondre) au domaine indiqué dans l'adresse d'origine. Si la politique DMARC du domaine spécifie un alignement strict pour le DKIM, ces domaines doivent correspondre exactement (SES utilise une politique DKIM stricte par défaut).

Pour se conformer à ces exigences, complétez les étapes suivantes :

- Configurez Easy DKIM en effectuant les procédures d' the section called “Easy DKIM”. Lorsque vous utilisez Easy DKIM, Amazon SES signe automatiquement vos e-mails.

> **Note**
>
> Plutôt que d'utiliser Easy DKIM, vous pouvez également signer manuellement vos messages. Cependant, vous devez être prudent si vous choisissez de le faire, car Amazon SES ne valide pas la signature DKIM que vous construisez. Pour cette raison, nous recommandons vivement d'utiliser Easy DKIM.

- Assurez-vous que le domaine spécifié dans la signature DKIM est aligné sur le domaine indiqué dans l'adresse d'origine. Ou, si vous envoyez depuis un sous-domaine du domaine indiqué dans l'adresse d'origine, assurez-vous que votre politique DMARC est définie de manière à assouplir l'alignement.

  > **Note**
  >
  > Vous pouvez déterminer l'alignement DMARC de votre domaine pour DKIM en tapant la commande suivante sur la ligne de commande et en remplaçant *example.com* par votre domaine :
  >
  > ```
  > dig -type=TXT _dmarc.example.com
  > ```
  >
  > Dans le résultat de la commande, sous Non-authoritative answer, recherchez un registre qui commence par `v=DMARC1`. Si cet registre inclut la chaîne `adkim=r`, ou si la chaîne `adkim` n'est pas du tout présente, votre domaine utilise l'alignement souple pour DKIM. Si le registre inclut la chaîne `adkim=s`, votre domaine utilise l'alignement strict pour DKIM. Votre administrateur système doit supprimer cette balise de le registre TXT DMARC dans la configuration DNS de votre domaine.
  > Vous pouvez également utiliser un outil de recherche DMARC basé sur le Web, tel que le DMARC Inspector sur le site Web de dmarcian ou l'outil de vérification DMARC sur le site MxToolBox Web, pour déterminer l'alignement des politiques de votre domaine pour le DKIM.

Utilisation de BIMI dans Amazon SES

BIMI (Brand Indicators for Message Identification, indicateurs de marque pour l'identification des messages) est une spécification de messagerie électronique qui permet aux boîtes de réception d'e-

mail d'afficher le logo d'une marque en regard des e-mails authentifiés de la marque dans les clients de messagerie compatibles.

En dépit de son lien direct avec l'authentification, la spécification de messagerie électronique BIMI n'est pas un protocole d'authentification de courrier électronique autonome dans le sens où elle exige que tous vos e-mails soient conformes à l'authentification DMARC.

Si BIMI exige DMARC, DMARC exige à son tour la présence d'enregistrements SPF ou DKIM dans votre domaine à des fins de conformité. Il est de toute façon préférable d'inclure des enregistrements SPF et DKIM pour une sécurité accrue et parce que certains fournisseurs de services de messagerie (ESP) exigent les deux lorsque BIMI est utilisé. La section suivante passe en revue les étapes d'implémentation de BIMI dans Amazon SES.

Configuration de BIMI dans SES

Vous pouvez configurer BIMI pour un domaine de messagerie qui vous appartient – dans la terminologie de SES, il s'agit d'un domaine MAIL FROM personnalisé. Une fois la configuration effectuée, tous les messages que vous enverrez depuis ce domaine afficheront votre logo BIMI dans les clients de messagerie qui prennent en charge BIMI.

Avant de pouvoir afficher un logo BIMI dans vos e-mails, vous devez cependant veiller à mettre en place certains éléments prérequis dans SES – dans la procédure suivante, ces prérequis sont généralisés et font référence à des sections dédiées qui traitent en détail ces sujets. Les étapes propres à BIMI et les éléments nécessaires à sa configuration dans SES sont détaillés ici.

Pour configurer BIMI sur un domaine MAIL FROM personnalisé

1. Vous devez disposer d'un domaine MAIL FROM personnalisé et l'avoir configuré dans SES avec des enregistrements SPF (de type TXT) et MX publiés pour ce même domaine. Si vous n'avez pas de domaine MAIL FROM personnalisé ou si vous souhaitez en créer un pour votre logo BIMI, consultez the section called “Utilisation d'un domaine MAIL FROM personnalisé”.
2. Configurez votre domaine avec Easy DKIM. Consultez the section called “Easy DKIM”.
3. Configurez votre domaine avec DMARC en publiant un enregistrement TXT auprès de votre fournisseur DNS avec les détails de politique d'application suivants exigés pour BIMI :

Nom	Type	Valeur
`_dmarc.example.com`	`TXT`	`v=DMARC1;p=quarantine;pct=100;rua=mailto:dmarcreports@example.com`
		`v=DMARC1;p=reject;rua=mailto:dmarcreports@example.com`

Dans l'exemple de politique DMARC précédent, comme l'exige BIMI :

- *`example.com`* doit être remplacé par votre nom de domaine ou de sous-domaine.
- La valeur de p= peut être :
  - quarantine avec une valeur de pct définie sur 100, comme indiqué, ou
  - reject comme indiqué.
- Si vos envois partent d'un sous-domaine, BIMI exige que le domaine parent intègre également cette politique d'application. Les sous-domaines seront soumis à la politique du domaine parent. Toutefois, si vous ajoutez un enregistrement DMARC pour votre sous-domaine en plus de ce que vous avez publié pour le domaine parent, votre sous-domaine doit également intégrer la même politique d'application pour être éligible à BIMI.
- Si vous n'avez jamais configuré de politique DMARC pour votre domaine, consultez the section called “Authentification d'e-mails avec DMARC” en veillant à n'utiliser que les valeurs de politique DMARC propres à BIMI, comme indiqué.

4. Produisez votre logo BIMI sous forme de fichier `.svg` (SVG, Scalable Vector Graphics) – le profil SVG spécifique exigé par BIMI est défini dans le format SVG P/S (SVG Portable/Secure). Pour que votre logo s'affiche dans le client de messagerie, il doit être parfaitement conforme à ces spécifications. Reportez-vous aux conseils de BIMI Group concernant la création de fichiers de logo SVG et les outils de conversion SVG recommandés.
5. (Facultatif) Procurez-vous un certificat VMC (Verified Mark Certificate). Certains ESP, tels que Gmail et Apple, vous demanderont un VMC pour prouver que vous êtes bien propriétaire de la marque et du contenu de votre logo BIMI. Même s'il ne s'agit pas d'une condition absolue pour implémenter BIMI sur votre domaine, si l'ESP auquel vous envoyez des e-mails applique la conformité VMC, votre logo BIMI ne s'affichera pas dans le client de messagerie. Consultez les

informations de référence de BIMI Group pour savoir auprès de quelles autorités de certification vous pouvez vous procurer un VMC pour votre logo.

6. Hébergez le fichier SVG de votre logo BIMI sur un serveur auquel vous avez accès pour le rendre accessible au public via HTTPS. Par exemple, vous pouvez le charger dans un compartiment Amazon S3.
7. Créez et publiez un enregistrement DNS BIMI qui comporte l'URL de votre logo. Lors de la vérification de votre enregistrement DMARC, un ESP qui prendre en charge BIMI recherchera également un enregistrement BIMI contenant l'URL du fichier `.svg` de votre logo, ainsi que l'URL du fichier `.pem` de votre VMC (si vous l'avez configuré). Si les enregistrements correspondent, votre logo BIMI s'affichera.

   Configurez votre domaine avec BIMI en publiant un enregistrement TXT auprès de votre fournisseur DNS avec les valeurs suivantes, comme indiqué – l'envoi depuis un domaine est représenté dans le premier exemple ; l'envoi depuis un sous-domaine est représenté dans le deuxième exemple :

Nom	Type	Valeur
`default._bimi.example.com`	TXT	`v=BIMI1;l=https://myhostingserver.com/images/logo.svg;a=https://myhostingserver.com/certificate/vmc_2023-01-01.pem`
`default._bimi.marketing.example.com`		

   Dans les exemples d'enregistrements BIMI précédents :

   - La valeur de nom doit textuellement spécifier `default._bimi.` en tant que sous-domaine de *`example.com`* ou *`marketing.example.com`* qui doit être remplacé par votre nom de domaine ou de sous-domaine.
   - La valeur de `v=` correspond à la version de l'enregistrement BIMI.
   - La valeur de `l=` correspond au logo représentant l'URL qui pointe vers le fichier `.svg` de votre image.
   - La valeur de `a=` correspond à l'autorité représentant l'URL qui pointe vers le fichier `.pem` de votre certificat.

Vous pouvez valider votre enregistrement BIMI à l'aide d'un outil tel que BIMI Inspector de BIMI Group.

La dernière étape de ce processus consiste à mettre en place une logique d'envoi régulier aux ESP qui prennent en charge le placement de logo BIMI. Votre domaine doit avoir une cadence de remise régulière et doit jouir d'une bonne réputation auprès des ESP auxquels vous envoyez des messages. Le logo BIMI peut prendre un certain temps avant d'être placé par les ESP si vous n'avez pas une réputation ou une cadence d'envoi bien établies.

Vous trouverez des informations et des ressources supplémentaires sur BIMI via l'organisation BIMI Group.

Configuration de notifications d'événement pour Amazon SES

Afin d'envoyer des e-mails avec Amazon SES, vous devez mettre en place un système de gestion des retours à l'expéditeur et des réclamations. Amazon SES peut vous informer des événements de retour à l'expéditeur ou de réclamation de trois manières : en envoyant un e-mail de notification, par notification dans une rubrique Amazon SNS ou en publiant des événements d'envoi. Cette section contient des informations sur la configuration d'Amazon SES pour envoyer certains types de notifications par e-mail ou notifier une rubrique Amazon SNS. Pour en savoir plus sur la publication d'événements d'envoi, consultez Surveillance de l'envoi d'e-mails à l'aide de la publication d'événements Amazon SES.

Vous pouvez configurer les notifications à l'aide de la console Amazon SES ou de l'API Amazon SES.

Rubriques

- Considérations Importantes
- Réception des notifications Amazon SES par e-mail
- Réception des notifications Amazon SES à l'aide d'Amazon SNS

Considérations Importantes

Il y a plusieurs points importants à prendre en compte lorsque vous configurez Amazon SES pour envoyer des notifications :

- Les notifications par e-mail et Amazon SNS s'appliquent aux identités individuelles (les adresses e-mail ou les domaines vérifiés que vous utilisez pour l'envoi des e-mails). Lorsque vous activez les notifications pour une identité, Amazon SES envoie uniquement les notifications pour les e-mails envoyés à partir de cette identité, et uniquement dans la région AWS dans laquelle vous avez configuré les notifications.
- Vous devez activer une méthode de réception des notifications de retour à l'expéditeur ou de réclamation. Vous pouvez envoyer des notifications à l'adresse de domaine ou e-mail qui a généré le retour à l'expéditeur ou la réclamation, ou à une rubrique Amazon SNS. Vous pouvez également utiliser la publication d'événements pour envoyer des notifications concernant différents types d'événements (notamment les rebonds, les plaintes, les livraisons, etc.) sur une rubrique Amazon SNS ou un stream Firehose.

  Si vous ne configurez pas l'une de ces méthodes de notifications de retour à l'expéditeur ou de réclamation, Amazon SES vous fait suivre automatiquement les notifications de retour à l'expéditeur et de réclamation par e-mail à l'adresse indiquée dans le champ Return-Path (Chemin de retour) (ou le champ Source, si vous n'avez pas spécifié d'adresse Return-Path (Chemin de retour)) du message qui a entraîné l'événement de retour à l'expéditeur ou de réclamation, même si vous avez désactivé le transfert de commentaires par e-mail.

  Si vous désactivez le transfert de commentaires par e-mail et que vous activiez la publication d'événements, vous devez également appliquer le jeu de configurations qui contient la règle de publication d'événements à chaque e-mail que vous envoyez. Dans ce cas, si vous n'utilisez pas le jeu de configurations, Amazon SES vous fait suivre automatiquement les notifications de retour à l'expéditeur et de réclamation à l'adresse Return-Path (Chemin de retour) ou Source de l'e-mail qui a entraîné l'événement de retour à l'expéditeur ou de réclamation.
- Si vous configurez Amazon SES pour envoyer des événements de retour à l'expéditeur et de réclamation à l'aide de plusieurs méthodes (par exemple, en envoyant des notifications par e-mail et en utilisant les événements d'envoi), vous pouvez recevoir plus d'une notification pour le même événement.

Réception des notifications Amazon SES par e-mail

Amazon SES peut vous envoyer un e-mail lorsque vous recevez des retours à l'expéditeur et des réclamations à l'aide d'un processus nommé transfert de commentaires par e-mail.

Afin d'envoyer des e-mails à l'aide d'Amazon SES, vous devez le configurer pour envoyer les notifications de retour à l'expéditeur et de réclamation à l'aide de l'une des méthodes suivantes :

- En activant le transfert de commentaires par e-mail. La procédure de configuration de ce type de notification est incluse dans cette section.
- En envoyant des notifications à une rubrique Amazon SNS. Pour de plus amples informations, veuillez consulter Réception des notifications Amazon SES à l'aide d'Amazon SNS.
- En publiant des notifications d'événement. Pour de plus amples informations, veuillez consulter Surveillance de l'envoi d'e-mails à l'aide de la publication d'événements Amazon SES.

> **Important**
>
> Pour prendre connaissance de plusieurs points importants relatifs aux notifications, consultez Configuration de notifications d'événement pour Amazon SES.

Rubriques

Activation du transfert de commentaires par e-mail

Le transfert de commentaires par e-mail est activé par défaut. Si vous l'avez désactivé précédemment, vous pouvez l'activer à l'aide des procédures de cette section.

Pour activer le transfert des notifications de retour à l'expéditeur et de réclamation par e-mail à l'aide de la console Amazon SES

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).
3. Dans la liste des adresses e-mail ou domaines vérifiés, choisissez l'adresse e-mail ou le domaine pour lequel vous souhaitez configurer des notifications de retour à l'expéditeur et de réclamation.
4. Dans le volet des détails, développez la section Notifications.
5. Choisissez Edit Configuration (Modifier la configuration).

6. Sous Email Feedback Forwarding (Destination du transfert de commentaires par e-mail), choisissez Enabled (Activé).

> **Note**
>
> Il peut se passer quelques minutes avant que les changements effectués sur cette page prennent effet.

Vous pouvez également activer les notifications de rebond et de réclamation par e-mail à l'aide de l'opération SetIdentityFeedbackForwardingEnabledAPI.

Désactivation du transfert de commentaires par e-mail

Si vous configurez une autre méthode pour fournir les notifications de retour à l'expéditeur et de réclamation, vous pouvez désactiver le transfert de commentaires par e-mail afin de ne pas recevoir plusieurs notifications lorsqu'un événement de retour à l'expéditeur ou de réclamation se produit.

Pour désactiver le transfert des notifications de retour à l'expéditeur et de réclamation par e-mail à l'aide de la console Amazon SES

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).
3. Dans la liste des adresses e-mail ou domaines vérifiés, choisissez l'adresse e-mail ou le domaine pour lequel vous souhaitez configurer des notifications de retour à l'expéditeur et de réclamation.
4. Dans le volet des détails, développez la section Notifications.
5. Choisissez Edit Configuration (Modifier la configuration).
6. Sous Email Feedback Forwarding (Destination du transfert de commentaires par e-mail), choisissez Disabled (Désactivé).

> **Note**
>
> Vous devez configurer une méthode de réception des notifications de retour à l'expéditeur et de réclamation pour envoyer des e-mails via Amazon SES. Si vous désactivez le transfert des commentaires par e-mail, vous devez activer les notifications

envoyées par Amazon SNS, ou publier les événements de rebond et de plainte sur une rubrique Amazon SNS ou un stream Firehose en utilisant la publication d'événements.
Si vous utilisez la publication d'événements, vous devez également appliquer le jeu de configurations qui contient la règle de publication d'événements à chaque e-mail que vous envoyez. Si vous n'avez pas configuré de méthode de réception des notifications de retour à l'expéditeur et de réclamation, Amazon SES vous fait suivre automatiquement les notifications de commentaires par e-mail à l'adresse indiquée dans le champ Return-Path (Chemin de retour) (Chemin de retour) (ou le champ Source si vous n'avez pas spécifié d'adresse Return-Path (Chemin de retour) (Chemin de retour)) du message qui a entraîné l'événement de retour à l'expéditeur ou de réclamation. Dans ce cas, Amazon SES transfère les notifications de retour à l'expéditeur et de réclamation, même si vous avez désactivé les notifications de commentaires par e-mail.

7. Choisissez Save Config (Enregistrer la configuration) pour enregistrer votre configuration de notifications.

> **Note**
>
> Il peut se passer quelques minutes avant que les changements effectués sur cette page prennent effet.

Vous pouvez également désactiver les notifications de rebond et de plainte par e-mail à l'aide de l'opération SetIdentityFeedbackForwardingEnabledAPI.

Destination du transfert de commentaires par e-mail

Lorsque vous recevez des notifications par e-mail, Amazon SES réécrit l'en-tête `From` et vous envoie la notification. L'adresse à laquelle Amazon SES transfère la notification dépend du moyen utilisé pour envoyer le message d'origine.

Si vous avez utilisé l'interface SMTP pour envoyer le message, les notifications sont remises selon les règles suivantes :

- Si vous avez spécifié un en-tête `Return-Path` dans la section `SMTP DATA`, les notifications sont envoyées à cette adresse.
- Sinon, les notifications sont envoyées à l'adresse que vous avez spécifiée lorsque vous avez émis la commande MAIL FROM.

Si vous avez utilisé l'opération d'API `SendEmail` pour envoyer le message, les notifications sont remises selon les règles suivantes :

- Si vous avez spécifié le paramètre `ReturnPath` facultatif dans votre appel à l'API `SendEmail`, les notifications sont envoyées à cette adresse.
- Sinon, les notifications sont envoyées à l'adresse définie dans le paramètre `Source` obligatoire de `SendEmail`.

Si vous avez utilisé l'opération d'API `SendRawEmail` pour envoyer le message, les notifications sont remises selon les règles suivantes :

- Si vous avez spécifié un en-tête `Return-Path` dans le message brut, les notifications sont envoyées à cette adresse.
- Sinon, si vous avez spécifié un paramètre `Source` dans votre appel à l'API `SendRawEmail`, les notifications sont envoyées à cette adresse.
- Sinon, les notifications sont envoyées à l'adresse indiquée dans l'en-tête `From` du message brut.

> **Note**
>
> Lorsque vous spécifiez une adresse `Return-Path` dans un e-mail, vous recevez les notifications à cette adresse. Toutefois, la version du message que le destinataire reçoit contient un en-tête `Return-Path` qui inclut une adresse e-mail anonyme (comme a0b1c2d3e4f5a6b7-c8d9e0f1-a2b3-c4d5-e6f7-a8b9c0d1e2f3-000000@amazonses.com). Cette anonymisation se produit, quelle que soit la façon dont vous avez envoyé l'e-mail.

Réception des notifications Amazon SES à l'aide d'Amazon SNS

Vous pouvez configurer Amazon SES de façon à notifier une rubrique Amazon SNS lorsque vous recevez des retours à l'expéditeur ou des réclamations, ou lorsque les e-mails sont remis. Les notifications Amazon SNS sont au format JavaScript Object Notation (JSON), ce qui vous permet de les traiter par programmation.

Afin d'envoyer des e-mails à l'aide d'Amazon SES, vous devez le configurer pour envoyer les notifications de retour et de réclamation à l'aide de l'une des méthodes suivantes :

- En envoyant des notifications à une rubrique Amazon SNS. La procédure de configuration de ce type de notification est incluse dans cette section.
- En activant le transfert de commentaires par e-mail. Pour plus d'informations, consultez Réception des notifications Amazon SES par e-mail.
- En publiant des notifications d'événement. Pour plus d'informations, consultez Surveillance de l'envoi d'e-mails à l'aide de la publication d'événements Amazon SES.

> **Important**
>
> Consultez Configuration de notifications d'événement pour Amazon SES pour obtenir des informations importantes sur les notifications.

Rubriques

Configuration des notifications Amazon SNS pour Amazon SES

Amazon SES peut vous informer de vos retours à l'expéditeur, réclamations et remises via Amazon Simple Notification Service (Amazon SNS).

Vous pouvez configurer des notifications dans la console Amazon SES ou à l'aide de l'API Amazon SES.

Rubriques de cette section :

Prérequis

Complétez les étapes suivantes avant de configurer des notifications Amazon SNS dans Amazon SES :

1. Créez une rubrique dans Amazon SNS. Pour en savoir plus, consultez Création d'une rubrique dans le Manuel du développeur d'Amazon Simple Notification Service.

> **Important**
>
> Lorsque vous créez votre rubrique à l'aide d'Amazon SNS, pour Type, choisissez uniquement Standard. (SES ne prend pas en charge les rubriques de type FIFO.)

Que vous créiez une nouvelle rubrique SNS ou sélectionniez une rubrique existante, vous devez donner un accès à SES pour publier des notifications sur la rubrique.

Pour donner à Amazon SES la permission de publier des notifications sur la rubrique, sur l'écran Edit topic (Modifier la rubrique) de la console SNS, développez Access policy (Stratégie d'accès) et dans JSON editor (Éditeur JSON), ajoutez la stratégie de l'autorisation suivante :

```
{
  "Version": "2012-10-17",
  "Id": "notification-policy",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ses.amazonaws.com"
      },
      "Action": "sns:Publish",
      "Resource": "arn:aws:sns:topic_region:111122223333:topic_name",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "111122223333",
          "AWS:SourceArn":
 "arn:aws:ses:topic_region:111122223333:identity/identity_name"
        }
      }
    }
  ]
}
```

Dans l'exemple précédent, apportez les modifications suivantes :

- Remplacez *topic_region* par la région AWS dans laquelle vous avez créé la rubrique SNS.

- Remplacez *111122223333* par votre ID de compte AWS.
- Remplacez *topic_name* par le nom de votre rubrique SNS.
- Remplacez *identity_name* par l'identité vérifiée (adresse e-mail ou domaine) que vous inscrivez à la rubrique SNS.

2. Abonnez au moins un point de terminaison pour la rubrique. Par exemple, si vous voulez recevoir des notifications par SMS, abonnez un point de terminaison SMS (c'est-à-dire, un numéro de téléphone portable) à la rubrique. Pour recevoir des notifications par e-mail, abonnez un point de terminaison de messagerie (une adresse e-mail) à la rubrique.

   Pour en savoir plus, consultez Mise en route dans le Guide du développeur Amazon Simple Notification Service.

3. (Facultatif) Si votre rubrique Amazon SNS utilise AWS Key Management Service (AWS KMS) pour le chiffrement côté serveur, vous devez ajouter des autorisations à la stratégie de clé AWS KMS. Vous pouvez ajouter des autorisations en attachant la stratégie suivante à la stratégie de clé AWS KMS :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSESToUseKMSKey",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

Configuration de notifications à l'aide de la console Amazon SES

Pour configurer des notifications à l'aide de la console Amazon SES

1. Ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).
3. Dans le conteneur Identities (Identités), sélectionnez l'identité vérifiée pour laquelle vous souhaitez recevoir des notifications de commentaires lorsqu'un message envoyé à partir de cette identité entraîne un retour à l'expéditeur, une réclamation ou une remise.

   > **Important**
   >
   > Les paramètres de notification de domaine vérifié s'appliquent à tous les e-mails envoyés depuis les adresses de ce domaine, à l'exception des adresses qui sont également vérifiées.

4. Dans l'écran de détails de l'identité vérifiée que vous avez sélectionnée, choisissez l'onglet Notifications (Notifications) et sélectionnez Edit (Modifier) dans le conteneur Feedback notifications (Notifications de commentaire).
5. Développez la zone de liste des rubriques SNS de chaque type de commentaires pour lequel vous souhaitez recevoir des notifications et sélectionnez soit une rubrique SNS dont vous êtes propriétaire, soit No SNS topic (Aucun sujet SNS), ou SNS topic you don't own (Sujet SNS dont vous n'êtes pas propriétaire).

   - Si vous avez choisi SNS topic you don't own (Sujet SNS dont vous n'êtes pas propriétaire), le champ ARN de rubrique SNS sera présenté et vous devrez entrer l'ARN de la rubrique SNS partagé avec vous par votre expéditeur délégué. (Seul l'expéditeur délégué recevra ces notifications, car il est propriétaire de la rubrique SNS. Pour en savoir plus sur l'envoi des délégués, consultez Présentation de l'autorisation d'envoi.)

   > **Important**
   >
   > Les rubriques Amazon SNS que vous utilisez pour les notifications de retour à l'expéditeur, de réclamation et de remise doivent se trouver dans la même Région AWS que celle utilisée dans Amazon SES.

De plus, vous devez abonner un ou plusieurs points de terminaison à la rubrique afin de recevoir des notifications. Par exemple, si vous voulez que des notifications soient envoyées à une adresse e-mail, vous devez abonner un point de terminaison de messagerie à la rubrique. Pour en savoir plus, consultez Mise en route dans le Guide du développeur Amazon Simple Notification Service.

6. (Facultatif) Si vous souhaitez que votre notification de rubrique inclue les en-têtes de l'e-mail d'origine, cochez la case Include original email headers (Incluez les en-têtes d'e-mail d'origine) située directement sous le nom de rubrique SNS de chaque type de commentaires. Cette option est disponible uniquement si vous avez affecté une rubrique Amazon SNS au type de notification associé. Pour en savoir plus sur le contenu des en-têtes de l'e-mail d'origine, consultez l'objet `mail` dans Contenu des notifications .
7. Choisissez Enregistrer les modifications. L'application des modifications que vous apportez à vos paramètres de notification peut prendre quelques minutes.
8. (Facultatif) Si vous avez choisi les notifications de rubriques Amazon SNS à la fois pour les retours à l'expéditeur et les réclamations, vous pouvez désactiver entièrement les notifications par e-mail afin de ne pas recevoir de doubles notifications par e-mail et par SNS. Pour désactiver les notifications par e-mail pour les retours à l'expéditeur et les réclamations, sous l'onglet Notifications (Notifications) sur l'écran de détails de l'identité vérifiée, dans le conteneur Email Feedback Forwarding (Transfert de commentaires par e-mail), choisissez Edit (Modifier), décochez la case Enabled (Activé), et choisissez Save changes (Enregistrer les modifications).

Une fois que vous avez configuré vos paramètres, vous allez commencer à recevoir des notifications de retour à l'expéditeur, de réclamation et/ou de remise, dans vos rubriques Amazon SNS. Ces notifications respectent le format JavaScript Object Notation (JSON) et suivent la structure décrite dans Contenu des notifications .

Vous serez facturé selon les tarifs Amazon SNS standard pour les notifications de retour à l'expéditeur, de réclamation et de remise. Pour en savoir plus, consultez la page Tarification d'Amazon SNS.

Note

Si une tentative de publication dans votre rubrique Amazon SNS échoue parce que la rubrique a été supprimée ou que votre Compte AWS n'est plus autorisé à publier dans celle-ci, Amazon SES supprime la configuration de cette rubrique si elle est configurée pour des retours à l'expéditeur ou des plaintes (pas des livraisons ; pour les notifications de livraison,

SES ne supprime pas le paramètre de configuration de rubrique SNS). De plus, Amazon SES réactive les notifications par e-mail de retour à l'expéditeur et de réclamation pour l'identité, et vous recevez une notification de modification par e-mail. Si plusieurs identités sont configurées pour utiliser la rubrique, la configuration de rubrique de chaque identité est modifiée lorsque l'identité ne parvient pas à publier dans la rubrique.

Configuration de notifications à l'aide de l'API Amazon SES

Vous pouvez également configurer des notifications de retour à l'expéditeur, de réclamation et de remise à l'aide de l'API Amazon SES. Utilisez les opérations suivantes pour configurer des notifications :

- SetIdentityNotificationTopic
- SetIdentityFeedbackForwardingEnabled
- GetIdentityNotificationAttributes
- SetIdentityHeadersInNotificationsEnabled

Vous pouvez utiliser ces actions d'API pour écrire une application frontale personnalisée pour les notifications. Pour une description complète des actions d'API liées aux notifications, consultez le document Amazon Simple Email Service API Reference.

Dépannage des notifications de commentaire

Pas de réception de notifications

Si vous ne recevez pas de notifications, vérifiez que vous avez abonné un point de terminaison à la rubrique via laquelle les notifications sont envoyées. Lorsque vous abonnez un point de terminaison de messagerie à une rubrique, vous recevez un e-mail vous demandant de confirmer votre abonnement. Vous devez confirmer votre abonnement avant de commencer à recevoir des notifications par e-mail. Pour en savoir plus, consultez Mise en route dans le Guide du développeur Amazon Simple Notification Service.

`InvalidParameterValue`Erreur lors du choix d'une rubrique

Si vous recevez une erreur indiquant qu'une erreur `InvalidParameterValue` s'est produite, vérifiez la rubrique Amazon SNS pour voir si elle est chiffrée via AWS KMS. Si c'est le cas, vous devez modifier la stratégie pour la clé AWS KMS. Consultez Prérequis pour obtenir un exemple de stratégie.

Contenu des notifications Amazon SNS pour Amazon SES

Les notifications de retour à l'expéditeur, de réclamation et de message délivré sont publiées dans les rubriques Amazon Simple Notification Service (Amazon SNS) au format JSON (JavaScript Object Notation). L'objet JSON de premier niveau contient une chaîne `notificationType`, un objet `mail` et un objet `bounce`, `complaint` ou `delivery`.

Consultez les sections suivantes Pour en savoir plus sur les différents types d'objets :

- Objet JSON de niveau supérieur
- Objet `mail`
- Objet `bounce`
- Objet `complaint`
- Objet `delivery`

Voici quelques remarques importantes sur le contenu des notifications Amazon SNS pour Amazon SES :

- Pour un type de notification donné, vous pouvez recevoir une notification Amazon SNS pour plusieurs destinataires, ou vous pouvez recevoir une seule notification Amazon SNS par destinataire. Votre code doit être en mesure d'analyser la notification Amazon SNS et de gérer les deux cas ; Amazon SES n'assure aucune garantie de classement ou de regroupement pour les notifications envoyées via Amazon SNS. Cependant, différents types de notification Amazon SNS (par exemple, retours à l'expéditeur et réclamations) ne sont pas combinés dans une même notification.
- Vous pouvez recevoir plusieurs types de notifications Amazon SNS pour un destinataire. Par exemple, le serveur de messagerie de réception peut accepter l'e-mail (déclenchement d'une notification de message livré), mais après le traitement de l'e-mail, le serveur de messagerie de réception peut déterminer que l'e-mail se traduit de fait par un retour à l'expéditeur (déclenchement d'une notification de retour à l'expéditeur). Cependant, ces notifications sont toujours distinctes, car ce sont des types de notification différents.
- Amazon SES se réserve le droit d'ajouter des champs supplémentaires aux notifications. À ce titre, les applications qui analysent ces notifications doivent être suffisamment flexible pour gérer les champs inconnus.
- Amazon SES remplace les en-têtes du message lors de l'envoi de l'e-mail. Vous trouverez les en-têtes du message d'origine dans les champs `headers` et `commonHeaders` de l'objet `mail`.

Objet JSON de niveau supérieur

L'objet JSON de niveau supérieur d'une notification Amazon SES contient les champs suivants.

Nom de champ	Description
`notificationType`	Chaîne qui contient le type de notification représenté par l'objet JSON. Les valeurs possibles sont `Bounce`, `Complaint` ou `Delivery`. Si vous configurez la publication d'événements, ce champ est nommé `eventType` .
`mail`	Objet JSON qui contient les informations sur l'e-mail d'origine auquel la notification s'applique. Pour plus d'informations, consultez Objet de l'e-mail.
`bounce`	Ce champ est disponible uniquement si le `notificationType` est `Bounce` et qu'il contient un objet JSON qui inclut les informations sur le retour à l'expéditeur. Pour plus d'informations, consultez Objet bounce.
`complaint`	Ce champ est disponible uniquement si le `notificationType` est `Complaint` et qu'il contient un objet JSON qui inclut les informations sur la réclamation. Pour plus d'informations, consultez Objet de réclamation.
`delivery`	Ce champ est disponible uniquement si le `notificationType` est `Delivery` et qu'il contient un objet JSON qui inclut les informations sur le message livré. Pour plus d'informations, consultez Objet Delivery.

Objet de l'e-mail

Chaque notification de retour à l'expéditeur, réclamation ou message délivré contient des informations sur l'e-mail d'origine dans l'objet `mail`. L'objet JSON qui contient les informations sur un objet `mail` comporte les champs suivants.

Nom de champ	Description
`timestamp`	Heure à laquelle le message a été envoyé (au format ISO8601).
`messageId`	ID unique attribué par Amazon SES au message. Amazon SES vous a renvoyé cette valeur lorsque vous avez envoyé le message. **Note** Cet ID de message a été attribué par Amazon SES. Vous trouverez l'ID de message de l'e-mail d'origine dans le champ `headers` de l'objet `mail`.
`source`	Adresse e-mail à partir de laquelle l'e-mail d'origine a été envoyé (adresse MAIL FROM de l'enveloppe).
`sourceArn`	ARN (Amazon Resource Name) de l'identité qui a été utilisée pour envoyer l'e-mail. Dans le cas d'une autorisation d'envoi, `sourceArn` correspond à l'ARN de l'identité dont le propriétaire a autorisé l'utilisation pour l'envoi de l'e-mail par l'expéditeur délégué. Pour en savoir plus sur l'autorisation d'envoi, consultez Méthodes d'authentification d'e-mail.
`sourceIp`	Adresse IP publique originale du client qui a effectué la demande d'envoi d'e-mail à Amazon SES.

Nom de champ	Description
`sendingAccountId`	ID Compte AWS du compte utilisé pour envoyer l'e-mail. Dans le cas de l'autorisation d'envoi, `sendingAccountId` correspond à l'ID de compte de l'expéditeur délégué.
`callerIdentity`	Identité IAM de l'utilisateur Amazon SES qui a envoyé l'e-mail.
`destination`	Liste des adresses e-mail destinataires de l'e-mail original.
`headersTruncated`	Cet objet ne s'affiche que si vous avez configuré les paramètres de notification en vue d'inclure les en-têtes de l'e-mail d'origine. Indique si les en-têtes sont tronqués dans la notification. Amazon SES tronque les en-têtes dans la notification lorsque les en-têtes du message d'origine ont une taille de 10 Ko ou plus. Les valeurs possibles sont `true` et `false`.

Nom de champ	Description
`headers`	Cet objet ne s'affiche que si vous avez configuré les paramètres de notification en vue d'inclure les en-têtes de l'e-mail d'origine. Liste des en-têtes d'origine de l'e-mail. Chaque en-tête de la liste a un champ `name` et un champ `value`. **Note** Tout ID de message de l'objet `headers` provient du message d'origine que vous avez transmis à Amazon SES. L'ID de message qu'Amazon SES a ensuite affecté au message se trouve dans le champ `messageId` de l'objet `mail`.

Nom de champ	Description
`commonHeaders`	Cet objet ne s'affiche que si vous avez configuré les paramètres de notification en vue d'inclure les en-têtes de l'e-mail d'origine. Comprend des informations sur les en-têtes d'e-mails courants dans l'e-mail d'origine, y compris les champs From (De), To (À) et Subject (Objet). Dans cet objet, chaque en-tête est une clé. Les champs From (De) et To (À) sont représentés par des tableaux qui peuvent contenir plusieurs valeurs. **Note** Pour les événements, tout ID de message contenu dans le champ `commonHeaders` correspond à l'ID de message qu'Amazon SES a par la suite affecté au message dans le champ `messageId` de l'objet mail. Les notifications contiendront l'ID de message de l'e-mail d'origine.

L'exemple suivant est un exemple d'objet `mail` qui contient les en-têtes de l'e-mail d'origine. Lorsque ce type de notification n'est pas configuré pour inclure les en-têtes de l'e-mail d'origine, l'objet `mail` n'inclut pas les champs `headersTruncated`, `headers` et `commonHeaders`.

```
{
   "timestamp":"2018-10-08T14:05:45 +0000",
   "messageId":"000001378603177f-7a5433e7-8edb-42ae-af10-f0181f34d6ee-000000",
   "source":"sender@example.com",
   "sourceArn": "arn:aws:ses:us-east-1:888888888888:identity/example.com",
   "sourceIp": "127.0.3.0",
   "sendingAccountId":"123456789012",
   "destination":[
```

```
      "recipient@example.com"
   ],
   "headersTruncated":false,
   "headers":[
      {
         "name":"From",
         "value":"\"Sender Name\" <sender@example.com>"
      },
      {
         "name":"To",
         "value":"\"Recipient Name\" <recipient@example.com>"
      },
      {
         "name":"Message-ID",
         "value":"custom-message-ID"
      },
      {
         "name":"Subject",
         "value":"Hello"
      },
      {
         "name":"Content-Type",
         "value":"text/plain; charset=\"UTF-8\""
      },
      {
         "name":"Content-Transfer-Encoding",
         "value":"base64"
      },
      {
         "name":"Date",
         "value":"Mon, 08 Oct 2018 14:05:45 +0000"
      }
   ],
   "commonHeaders":{
      "from":[
         "Sender Name <sender@example.com>"
      ],
      "date":"Mon, 08 Oct 2018 14:05:45 +0000",
      "to":[
         "Recipient Name <recipient@example.com>"
      ],
      "messageId":" custom-message-ID",
      "subject":"Message sent using Amazon SES"
   }
```

```
}
```

Objet bounce

L'objet JSON qui contient les informations sur les retours à l'expéditeur comporte les champs suivants.

Nom de champ	Description
`bounceType`	Type de retour à l'expéditeur, tel que déterminé par Amazon SES. Pour plus d'informations, consultez Types de retour à l'expéditeur.
`bounceSubType`	Sous-type de retour à l'expéditeur, tel que déterminé par Amazon SES. Pour plus d'informations, consultez Types de retour à l'expéditeur.
`bouncedRecipients`	Liste qui contient les informations sur les destinataires de l'e-mail d'origine ayant fait l'objet d'un retour à l'expéditeur. Pour plus d'informations, consultez Destinataires à l'origine d'un retour à l'expéditeur.
`timestamp`	Date et heure auxquelles le retour à l'expédit eur a été envoyé (au format ISO8601). Notez qu'il s'agit de l'heure à laquelle la notification a été envoyée par le FAI, et non de l'heure à laquelle elle a été reçue par Amazon SES.
`feedbackId`	ID unique du retour à l'expéditeur.

Si Amazon SES a été en mesure de contacter l'autorité de transfert des messages à distance (MTA), le champ suivant est également présent.

Nom de champ	Description
`remoteMtaIp`	Adresse IP de la MTA à laquelle Amazon SES a tenté de remettre l'e-mail.

Si une notification de statut de remise (DSN) a été attachée au retour à l'expéditeur, le champ suivant est également présent.

Nom de champ	Description
`reportingMTA`	Valeur du champ `Reporting-MTA` du DSN. Il s'agit de la valeur de la MTA qui a tenté d'effectuer l'opération de remise, de relais ou de passerelle décrite dans le DSN.

Voici un exemple d'objet `bounce`.

```
{
   "bounceType":"Permanent",
   "bounceSubType": "General",
   "bouncedRecipients":[
      {
         "status":"5.0.0",
         "action":"failed",
         "diagnosticCode":"smtp; 550 user unknown",
         "emailAddress":"recipient1@example.com"
      },
      {
         "status":"4.0.0",
         "action":"delayed",
         "emailAddress":"recipient2@example.com"
      }
   ],
   "reportingMTA": "example.com",
   "timestamp":"2012-05-25T14:59:38.605Z",
   "feedbackId":"000001378603176d-5a4b5ad9-6f30-4198-a8c3-b1eb0c270a1d-000000",
   "remoteMtaIp":"127.0.2.0"
}
```

Destinataires à l'origine d'un retour à l'expéditeur

Une notification de retour à l'expéditeur peut se rapporter à un seul destinataire ou à plusieurs destinataires. Le champ `bouncedRecipients` contient une liste d'objets (un objet par destinataire auquel la notification de retour à l'expéditeur s'applique), ainsi que le champ suivant.

Nom de champ	Description
`emailAddress`	Adresse e-mail du destinataire. Si un DSN est disponible, l'adresse correspond à la valeur du champ `Final-Recipient` du DSN.

En outre, si un DSN est attaché au retour à l'expéditeur, les champs suivants peuvent également être présents.

Nom de champ	Description
`action`	Valeur du champ `Action` du DSN. Cette valeur indique l'action effectuée par la MTA de suivi comme résultat de sa tentative de remettre le message à ce destinataire.
`status`	Valeur du champ `Status` du DSN. Il s'agit du code de statut indépendant du transport par destinataire qui indique le statut de remise du message.
`diagnosticCode`	Code de statut émis par la MTA de suivi. Il s'agit de la valeur du champ `Diagnostic-Code` du DSN. Ce champ peut être absent du DSN (et donc également absent du JSON).

Voici un exemple d'objet qui pourrait être dans la liste `bouncedRecipients`.

```
{
    "emailAddress": "recipient@example.com",
    "action": "failed",
```

```
    "status": "5.0.0",
    "diagnosticCode": "X-Postfix; unknown user"
}
```

Types de retour à l'expéditeur

L'objet de retour à l'expéditeur contient un type `Undetermined`, `Permanent` ou `Transient`. Les types de retour à l'expéditeur `Permanent` et `Transient` peuvent également contenir l'un des nombreux sous-types de retour à l'expéditeur.

Lorsque vous recevez une notification de retour à l'expéditeur avec un type de retour à l'expéditeur `Transient`, il se peut que vous puissiez à l'avenir envoyer un e-mail à ce destinataire si le problème à l'origine du message de retour à l'expéditeur a été résolu.

Lorsque vous recevez une notification de retour à l'expéditeur avec un type de retour à l'expéditeur `Permanent`, il est peu probable que vous soyez en mesure à l'avenir d'envoyer des e-mails à ce destinataire. Pour cette raison, vous devez supprimer immédiatement de vos listes de diffusion le destinataire dont l'adresse a généré le retour à l'expéditeur.

> **Note**
>
> Lorsqu'un message d'erreur temporaire (un retour à l'expéditeur lié à un problème temporaire, tel que la boîte de réception du destinataire est pleine) se produit, Amazon SES tente de remettre à nouveau l'e-mail pendant une certaine période de temps. À la fin de cette période, si Amazon SES ne parvient toujours pas à remettre l'e-mail, il cesse d'essayer. Amazon SES fournit des notifications pour les retours à l'expéditeur définitifs, ainsi que pour les retours à l'expéditeur temporaires, selon lesquelles il a cessé d'essayer de remettre. Si vous souhaitez recevoir une notification chaque fois qu'un message d'erreur temporaire se produit, activez la publication d'événements et configurez-la pour envoyer des notifications lorsque des événements de retard de livraison se produisent.

bounceType	bounceSubType	Description
`Undetermined`	`Undetermined`	Le fournisseur de messagerie du destinataire a envoyé un message de retour à l'expéditeur. Le message de retour à l'expéditeur ne contenait pas suffisamment d'informations pour

bounceType	bounceSubType	Description
		qu'Amazon SES puisse déterminer la raison du retour à l'expéditeur. L'e-mail de retour à l'expéditeur, qui a été envoyé à l'adresse indiquée dans l'en-tête Return-Path (Chemin de retour) de l'e-mail à l'origine du retour à l'expéditeur, peut contenir des informations supplémentaires sur le problème qui a entraîné le retour de l'e-mail à l'expéditeur.
`Permanent`	`General`	Le fournisseur de messagerie du destinataire a envoyé un message d'erreur définitif. **Important** Lorsque vous recevez ce type de notification de retour à l'expédit eur, vous devez aussitôt supprimer l'adresse e-mail du destinataire de votre liste de diffusion. L'envoi de messages à des adresses qui produisent des messages d'erreur définitifs peut avoir un impact négatif sur votre réputatio n d'expéditeur. Si vous continuez d'envoyer des e-mails à des adresses qui produisent des messages d'erreur définitifs, nous pouvons suspendre votre capacité à envoyer de nouveaux e-mails. Consultez the section called “Utilisation de la liste de suppression au niveau du compte”.
`Permanent`	`NoEmail`	Il n'a pas été possible de récupérer l'adresse e-mail du destinataire dans le message de retour.

bounceType	bounceSubType	Description
`Permanent`	`Suppressed`	L'adresse e-mail du destinataire est sur la liste de suppression Amazon SES, car elle a un historique récent montrant qu'elle génère des messages d'erreur définitifs. Pour remplacer la liste de suppression globale, consultez Utilisation de la liste de suppression au niveau du compte Amazon SES.
`Permanent`	`OnAccountSuppressionList`	Amazon SES a supprimé l'envoi à cette adresse car celle-ci figure dans la liste de suppression au niveau du compte. Cela n'est pas pris en compte dans votre métrique de taux de retours à l'expéditeur.
`Transient`	`General`	Le fournisseur de messagerie du destinataire a envoyé un message de retour à l'expéditeur général. Il se peut que vous soyez en mesure d'envoyer à l'avenir un message au même destinataire si le problème qui a provoqué le retour du message à l'expéditeur est résolu. **Note** Si vous envoyez un e-mail à un destinataire qui possède une règle de réponse automatique active (comme un message « Absent du bureau » message), vous pouvez recevoir ce type de notification. Même si la réponse possède un type de notification `Bounce`, Amazon SES ne comptabilise pas les réponses automatiques lorsqu'il calcule le taux de retours à l'expéditeur pour votre compte.

bounceType	bounceSubType	Description
Transient	MailboxFull	Le fournisseur de messagerie du destinataire a envoyé un message de retour à l'expéditeur, car la boîte de réception du destinataire était pleine. Il se peut que vous puissiez à l'avenir envoyer le message au même destinataire lorsque la boîte de réception ne sera plus pleine.
Transient	MessageTooLarge	Le fournisseur de messagerie du destinataire a envoyé un message de retour à l'expéditeur, car le message envoyé était trop volumineux. Vous pouvez réessayer l'envoi à ce destinataire si vous réduisez la taille du message.
Transient	ContentRejected	Le fournisseur de messagerie du destinataire a envoyé un message de retour à l'expéditeur, car le message que vous avez envoyé comporte un contenu que le fournisseur n'autorise pas. Vous pouvez réessayer l'envoi du message au destinataire si vous modifiez le contenu du message.
Transient	AttachmentRejected	Le fournisseur de messagerie du destinataire a envoyé un message de retour à l'expéditeur, car le message contenait une pièce jointe indésirable. Par exemple, certains fournisseurs de messagerie peuvent rejeter des messages avec des pièces jointes d'un certain type de fichier ou des messages avec pièces jointes très volumineuses. Vous pouvez réessayer l'envoi du message au destinataire si vous supprimez ou modifiez le contenu de la pièce jointe.

Objet de réclamation

L'objet JSON qui contient les informations sur les réclamations comporte les champs suivants.

Nom de champ	Description
`complainedRecipients`	Liste contenant des informations sur les destinataires qui sont responsables de la réclamation. Pour plus d'informations, consultez Destinataires à l'origine d'une réclamation.
`timestamp`	Date et heure auxquelles le fournisseur de services Internet a envoyé la notification de réclamation, au format ISO8601. Les date et heure du champ peuvent ne pas être les mêmes que celles auxquelles Amazon SES a reçu la notification.
`feedbackId`	ID unique associé à la réclamation.
`complaintSubType`	La valeur du champ `complaintSubType` peut être null ou `OnAccountSuppressionList` . Si la valeur est `OnAccountSuppressionList` , Amazon SES a accepté le message, mais n'a pas essayé de l'envoyer car elle figurait dans la liste de suppression au niveau du compte.

De plus, si un rapport de commentaire est attaché à la réclamation, les champs suivants peuvent être présents.

Nom de champ	Description
`userAgent`	Valeur du champ `User-Agent` du rapport de commentaires. Cette valeur indique le nom et la version du système ayant généré le rapport.

Nom de champ	Description
`complaintFeedbackType`	Valeur du champ `Feedback-Type` du rapport de commentaires reçu de l'ISP. La valeur contient le type de commentaires.
`arrivalDate`	Valeur du champ `Arrival-Date` ou `Received-Date` du rapport de commentaires (au format ISO8601). Le champ peut être absent du rapport (et donc également absent du JSON).

Voici un exemple d'objet `complaint`.

```
{
   "userAgent":"ExampleCorp Feedback Loop (V0.01)",
   "complainedRecipients":[
      {
         "emailAddress":"recipient1@example.com"
      }
   ],
   "complaintFeedbackType":"abuse",
   "arrivalDate":"2009-12-03T04:24:21.000-05:00",
   "timestamp":"2012-05-25T14:59:38.623Z",
   "feedbackId":"000001378603177f-18c07c78-fa81-4a58-9dd1-fedc3cb8f49a-000000"
}
```

Destinataires à l'origine d'une réclamation

Le champ `complainedRecipients` contient la liste des destinataires susceptibles d'avoir déposé la réclamation. Vous devez utiliser ces informations pour déterminer quel destinataire est à l'origine de la réclamation, puis supprimer immédiatement ce destinataire de vos listes de diffusion.

> **Important**
>
> La plupart des fournisseurs de services Internet suppriment l'adresse e-mail du destinataire à l'origine de la réclamation de la notification de réclamation. Pour cette raison, la liste contient les informations sur les destinataires susceptibles d'avoir envoyé la réclamation, en

fonction des destinataires du message d'origine et du FAI duquel la réclamation a été reçue. Amazon SES effectue une recherche sur le message d'origine afin de déterminer la liste des destinataires.

Les objets JSON de cette liste contiennent le champ suivant.

Nom de champ	Description
`emailAddress`	Adresse e-mail du destinataire.

Voici un exemple d'objet destinataire à l'origine d'une réclamation.

```
{ "emailAddress": "recipient1@example.com" }
```

> **Note**
>
> En raison de ce comportement, vous êtes plus à même de savoir quelles adresses e-mail ont porté réclamation contre votre message si vous limitez l'envoi à un message par destinataire (plutôt que d'envoyer un message avec 30 adresses différentes dans la ligne Cci).

Types de réclamation

Vous pouvez voir les types de réclamation suivants dans le champ `complaintFeedbackType` tels qu'attribués par l'ISP du rapport, selon le site web IANA (Internet Assigned Numbers) :

- `abuse` – Indique un e-mail indésirable ou autre type d'e-mail malveillant.
- `auth-failure` – Rapport d'échec d'authentification d'e-mail.
- `fraud` – Indique certains types de fraude ou d'activité d'hameçonnage.
- `not-spam` – Indique que l'entité qui fournit le rapport ne considère pas le message en tant que courrier indésirable. Cette option permet de corriger un message qui a été mal balisé ou classé à tort comme courrier indésirable.
- `other` – Indique tout autre commentaire ne pouvant être classé dans les autres types enregistrés.
- `virus` – Signale qu'un virus a été détecté dans le message d'origine.

Objet Delivery

L'objet JSON qui contient les informations sur les messages remis comporte les champs suivants.

Nom de champ	Description
`timestamp`	Heure à laquelle Amazon SES a remis l'e-mail au serveur de messagerie du destinataire (au format ISO8601).
`processingTimeMillis`	Délai, en millisecondes, entre le moment où Amazon SES a accepté la demande de l'expéditeur et celui où le message a été transmis au serveur de messagerie du destinataire.
`recipients`	Liste des destinataires prévus de l'e-mail auxquels la notification de remise s'applique.
`smtpResponse`	Message de réponse SMTP du FAI distant ayant accepté l'e-mail depuis Amazon SES. Ce message varie selon l'e-mail, le serveur de messagerie de réception et l'ISP de réception.
`reportingMTA`	Nom d'hôte du serveur de messagerie Amazon SES ayant envoyé l'e-mail.
`remoteMtaIp`	Adresse IP de la MTA à laquelle Amazon SES a remis l'e-mail.

Voici un exemple d'objet `delivery`.

```
{
   "timestamp":"2014-05-28T22:41:01.184Z",
   "processingTimeMillis":546,
   "recipients":["success@simulator.amazonses.com"],
   "smtpResponse":"250 ok:  Message 64111812 accepted",
   "reportingMTA":"a8-70.smtp-out.amazonses.com",
   "remoteMtaIp":"127.0.2.0"
```

```
}
```

Exemples de notification Amazon SNS pour Amazon SES

Les sections suivantes fournissent des exemples pour les trois types de notification :

- Pour des exemples de notification de retour à l'expéditeur, consultez Exemples de notification de retour à l'expéditeur Amazon SNS.
- Pour des exemples de notification de réclamation, consultez Exemples de notification de réclamation Amazon SNS.
- Pour des exemples de notification de remise, consultez Exemple de notification de remise Amazon SNS.

Exemples de notification de retour à l'expéditeur Amazon SNS

Cette section contient des exemples de notification de retour à l'expéditeur avec et sans notification de statut de remise (DSN) fourni par le destinataire de l'e-mail ayant envoyé le commentaire.

Notification de retour à l'expéditeur avec une DSN

L'exemple suivant illustre une notification de retour à l'expéditeur qui contient une DSN et les en-têtes de l'e-mail d'origine. Lorsque les notifications de retour à l'expéditeur ne sont pas configurées pour inclure les en-têtes de l'e-mail d'origine, l'objet `mail` des notifications n'inclut pas les champs `headersTruncated`, `headers` et `commonHeaders`.

```
{
    "notificationType":"Bounce",
    "bounce":{
       "bounceType":"Permanent",
       "reportingMTA":"dns; email.example.com",
       "bouncedRecipients":[
          {
             "emailAddress":"jane@example.com",
             "status":"5.1.1",
             "action":"failed",
             "diagnosticCode":"smtp; 550 5.1.1 <jane@example.com>... User"
          }
       ],
       "bounceSubType":"General",
       "timestamp":"2016-01-27T14:59:38.237Z",
       "feedbackId":"00000138111222aa-33322211-cccc-cccc-cccc-ddddaaaa068a-000000",
```

```
         "remoteMtaIp":"127.0.2.0"
      },
      "mail":{
         "timestamp":"2016-01-27T14:59:38.237Z",
         "source":"john@example.com",
         "sourceArn": "arn:aws:ses:us-east-1:888888888888:identity/example.com",
         "sourceIp": "127.0.3.0",
         "sendingAccountId":"123456789012",
         "callerIdentity": "IAM_user_or_role_name",
         "messageId":"00000138111222aa-33322211-cccc-cccc-cccc-ddddaaaa0680-000000",
         "destination":[
           "jane@example.com",
           "mary@example.com",
           "richard@example.com"],
         "headersTruncated":false,
         "headers":[
          {
            "name":"From",
            "value":"\"John Doe\" <john@example.com>"
          },
          {
            "name":"To",
            "value":"\"Jane Doe\" <jane@example.com>, \"Mary Doe\" <mary@example.com>,
\"Richard Doe\" <richard@example.com>"
          },
          {
            "name":"Message-ID",
            "value":"custom-message-ID"
          },
          {
            "name":"Subject",
            "value":"Hello"
          },
          {
            "name":"Content-Type",
            "value":"text/plain; charset=\"UTF-8\""
          },
          {
            "name":"Content-Transfer-Encoding",
            "value":"base64"
          },
          {
            "name":"Date",
            "value":"Wed, 27 Jan 2016 14:05:45 +0000"
```

```
          }
         ],
         "commonHeaders":{
            "from":[
               "John Doe <john@example.com>"
            ],
            "date":"Wed, 27 Jan 2016 14:05:45 +0000",
            "to":[
               "Jane Doe <jane@example.com>, Mary Doe <mary@example.com>, Richard Doe
<richard@example.com>"
            ],
            "messageId":"custom-message-ID",
            "subject":"Hello"
          }
       }
   }
```

Notification de retour à l'expéditeur sans DSN

L'exemple suivant illustre une notification de retour à l'expéditeur qui contient les en-têtes de l'e-mail d'origine, mais pas de DSN. Lorsque les notifications de retour à l'expéditeur ne sont pas configurées pour inclure les en-têtes de l'e-mail d'origine, l'objet `mail` des notifications n'inclut pas les champs `headersTruncated`, `headers` et `commonHeaders`.

```
  {
     "notificationType":"Bounce",
     "bounce":{
        "bounceType":"Permanent",
        "bounceSubType": "General",
        "bouncedRecipients":[
           {
              "emailAddress":"jane@example.com"
           },
           {
              "emailAddress":"richard@example.com"
           }
        ],
        "timestamp":"2016-01-27T14:59:38.237Z",
        "feedbackId":"00000137860315fd-869464a4-8680-4114-98d3-716fe35851f9-000000",
        "remoteMtaIp":"127.0.2.0"
     },
     "mail":{
        "timestamp":"2016-01-27T14:59:38.237Z",
```

```
        "messageId":"00000137860315fd-34208509-5b74-41f3-95c5-22c1edc3c924-000000",
        "source":"john@example.com",
        "sourceArn": "arn:aws:ses:us-east-1:888888888888:identity/example.com",
        "sourceIp": "127.0.3.0",
        "sendingAccountId":"123456789012",
        "callerIdentity": "IAM_user_or_role_name",
        "destination":[
           "jane@example.com",
           "mary@example.com",
           "richard@example.com"
        ],
       "headersTruncated":false,
       "headers":[
        {
           "name":"From",
           "value":"\"John Doe\" <john@example.com>"
        },
        {
           "name":"To",
           "value":"\"Jane Doe\" <jane@example.com>, \"Mary Doe\" <mary@example.com>,
\"Richard Doe\" <richard@example.com>"
        },
        {
           "name":"Message-ID",
           "value":"custom-message-ID"
        },
        {
           "name":"Subject",
           "value":"Hello"
        },
        {
           "name":"Content-Type",
           "value":"text/plain; charset=\"UTF-8\""
        },
        {
           "name":"Content-Transfer-Encoding",
           "value":"base64"
        },
        {
           "name":"Date",
           "value":"Wed, 27 Jan 2016 14:05:45 +0000"
         }
        ],
        "commonHeaders":{
```

```
          "from":[
             "John Doe <john@example.com>"
          ],
          "date":"Wed, 27 Jan 2016 14:05:45 +0000",
          "to":[
             "Jane Doe <jane@example.com>, Mary Doe <mary@example.com>, Richard Doe
<richard@example.com>"
          ],
          "messageId":"custom-message-ID",
          "subject":"Hello"
       }
    }
 }
```

Exemples de notification de réclamation Amazon SNS

Cette section contient des exemples de notification de réclamation avec et sans rapport de commentaire fourni par le destinataire de l'e-mail ayant envoyé le commentaire.

Notification de réclamation avec un rapport de commentaire

L'exemple suivant illustre une notification de réclamation qui contient un rapport de commentaire et les en-têtes de l'e-mail d'origine. Lorsque les notifications de réclamation ne sont pas configurées pour inclure les en-têtes de l'e-mail d'origine, l'objet `mail` des notifications n'inclut pas les champs `headersTruncated`, `headers` et `commonHeaders`.

```
  {
     "notificationType":"Complaint",
     "complaint":{
        "userAgent":"AnyCompany Feedback Loop (V0.01)",
        "complainedRecipients":[
           {
              "emailAddress":"richard@example.com"
           }
        ],
        "complaintFeedbackType":"abuse",
        "arrivalDate":"2016-01-27T14:59:38.237Z",
        "timestamp":"2016-01-27T14:59:38.237Z",
        "feedbackId":"000001378603177f-18c07c78-fa81-4a58-9dd1-fedc3cb8f49a-000000"
     },
     "mail":{
        "timestamp":"2016-01-27T14:59:38.237Z",
        "messageId":"000001378603177f-7a5433e7-8edb-42ae-af10-f0181f34d6ee-000000",
```

```
        "source":"john@example.com",
        "sourceArn": "arn:aws:ses:us-east-1:888888888888:identity/example.com",
        "sourceIp": "127.0.3.0",
        "sendingAccountId":"123456789012",
        "callerIdentity": "IAM_user_or_role_name",
        "destination":[
           "jane@example.com",
           "mary@example.com",
           "richard@example.com"
        ],
         "headersTruncated":false,
         "headers":[
          {
            "name":"From",
            "value":"\"John Doe\" <john@example.com>"
          },
          {
            "name":"To",
            "value":"\"Jane Doe\" <jane@example.com>, \"Mary Doe\" <mary@example.com>,
\"Richard Doe\" <richard@example.com>"
          },
          {
            "name":"Message-ID",
            "value":"custom-message-ID"
          },
          {
            "name":"Subject",
            "value":"Hello"
          },
          {
            "name":"Content-Type",
            "value":"text/plain; charset=\"UTF-8\""
          },
          {
            "name":"Content-Transfer-Encoding",
            "value":"base64"
          },
          {
            "name":"Date",
            "value":"Wed, 27 Jan 2016 14:05:45 +0000"
          }
        ],
        "commonHeaders":{
          "from":[
```

```
            "John Doe <john@example.com>"
         ],
         "date":"Wed, 27 Jan 2016 14:05:45 +0000",
         "to":[
            "Jane Doe <jane@example.com>, Mary Doe <mary@example.com>, Richard Doe
<richard@example.com>"
         ],
         "messageId":"custom-message-ID",
         "subject":"Hello"
      }
   }
}
```

Notification de réclamation sans rapport de commentaire

L'exemple suivant illustre une notification de réclamation qui contient les en-têtes de l'e-mail d'origine, mais pas de rapport de commentaire. Lorsque les notifications de réclamation ne sont pas configurées pour inclure les en-têtes de l'e-mail d'origine, l'objet `mail` des notifications n'inclut pas les champs `headersTruncated`, `headers` et `commonHeaders`.

```
{
   "notificationType":"Complaint",
   "complaint":{
      "complainedRecipients":[
         {
            "emailAddress":"richard@example.com"
         }
      ],
      "timestamp":"2016-01-27T14:59:38.237Z",
      "feedbackId":"0000013786031775-fea503bc-7497-49e1-881b-a0379bb037d3-000000"
   },
   "mail":{
      "timestamp":"2016-01-27T14:59:38.237Z",
      "messageId":"0000013786031775-163e3910-53eb-4c8e-a04a-f29debf88a84-000000",
      "source":"john@example.com",
      "sourceArn": "arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "sourceIp": "127.0.3.0",
      "sendingAccountId":"123456789012",
      "callerIdentity": "IAM_user_or_role_name",
      "destination":[
         "jane@example.com",
         "mary@example.com",
         "richard@example.com"
```

```
        ],
        "headersTruncated":false,
        "headers":[
         {
           "name":"From",
           "value":"\"John Doe\" <john@example.com>"
         },
         {
           "name":"To",
           "value":"\"Jane Doe\" <jane@example.com>, \"Mary Doe\" <mary@example.com>,
\"Richard Doe\" <richard@example.com>"
         },
         {
           "name":"Message-ID",
           "value":"custom-message-ID"
         },
         {
           "name":"Subject",
           "value":"Hello"
         },
         {
           "name":"Content-Type",
           "value":"text/plain; charset=\"UTF-8\""
         },
         {
           "name":"Content-Transfer-Encoding",
           "value":"base64"
         },
         {
           "name":"Date",
           "value":"Wed, 27 Jan 2016 14:05:45 +0000"
         }
         ],
         "commonHeaders":{
            "from":[
               "John Doe <john@example.com>"
            ],
            "date":"Wed, 27 Jan 2016 14:05:45 +0000",
            "to":[
               "Jane Doe <jane@example.com>, Mary Doe <mary@example.com>, Richard Doe
<richard@example.com>"
            ],
            "messageId":"custom-message-ID",
            "subject":"Hello"
```

```
        }
     }
}
```

Exemple de notification de remise Amazon SNS

L'exemple suivant illustre une notification de remise qui contient les en-têtes de l'e-mail d'origine. Lorsque les notifications de remise ne sont pas configurées pour inclure les en-têtes de l'e-mail d'origine, l'objet `mail` des notifications n'inclut pas les champs `headersTruncated`, `headers` et `commonHeaders`.

```
{
   "notificationType":"Delivery",
   "mail":{
      "timestamp":"2016-01-27T14:59:38.237Z",
      "messageId":"0000014644fe5ef6-9a483358-9170-4cb4-a269-f5dcdf415321-000000",
      "source":"john@example.com",
      "sourceArn": "arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "sourceIp": "127.0.3.0",
      "sendingAccountId":"123456789012",
      "callerIdentity": "IAM_user_or_role_name",
      "destination":[
         "jane@example.com"
      ],
       "headersTruncated":false,
       "headers":[
        {
           "name":"From",
           "value":"\"John Doe\" <john@example.com>"
        },
        {
           "name":"To",
           "value":"\"Jane Doe\" <jane@example.com>"
        },
        {
           "name":"Message-ID",
           "value":"custom-message-ID"
        },
        {
           "name":"Subject",
           "value":"Hello"
        },
        {
```

```
            "name":"Content-Type",
            "value":"text/plain; charset=\"UTF-8\""
         },
         {
            "name":"Content-Transfer-Encoding",
            "value":"base64"
         },
         {
            "name":"Date",
            "value":"Wed, 27 Jan 2016 14:58:45 +0000"
         }
        ],
        "commonHeaders":{
          "from":[
             "John Doe <john@example.com>"
          ],
          "date":"Wed, 27 Jan 2016 14:58:45 +0000",
          "to":[
             "Jane Doe <jane@example.com>"
          ],
          "messageId":"custom-message-ID",
          "subject":"Hello"
        }
     },
    "delivery":{
       "timestamp":"2016-01-27T14:59:38.237Z",
       "recipients":["jane@example.com"],
       "processingTimeMillis":546,
       "reportingMTA":"a8-70.smtp-out.amazonses.com",
       "smtpResponse":"250 ok:  Message 64111812 accepted",
       "remoteMtaIp":"127.0.2.0"
    }
}
```

Utilisation de l'autorisation d'identité dans Amazon SES

Les stratégies d'autorisation des identités définissent comment les identités individuelles vérifiées peuvent utiliser Amazon SES en spécifiant quelles actions de l'API SES sont autorisées ou refusées pour l'identité et dans quelles conditions.

Grâce à l'utilisation de ces stratégies d'autorisation, vous pouvez garder le contrôle de vos identités en modifiant ou en révoquant les autorisations à tout moment. Vous pouvez même autoriser d'autres

utilisateurs à utiliser les identités que vous possédez (domaines ou adresses e-mail) avec leurs propres comptes SES.

Rubriques

Anatomie de la stratégie Amazon SES

Les stratégies respectent une structure spécifique, contiennent des éléments et doivent répondre à certaines exigences.

Structure d'une politique

Chaque stratégie d'autorisation est un document JSON attaché à une identité. Chaque stratégie comprend les sections suivantes :

- Les informations à l'échelle de la stratégie en haut du document.
- Une ou plusieurs instructions individuelles, chacune décrivant un ensemble d'autorisations.

L'exemple de politique suivant accorde au compte AWS possédant l'ID 123456789012 les autorisations spécifiées dans la section Action pour le domaine vérifié example.com.

```
{
  "Id":"ExampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeAccount",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:123456789012:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
      "Action":[
```

```
        "ses:GetEmailIdentity",
        "ses:UpdateEmailIdentityPolicy",
        "ses:ListRecommendations",
        "ses:CreateEmailIdentityPolicy",
        "ses:DeleteEmailIdentity"
      ]
    }
  ]
}
```

Vous pouvez trouver d'autres exemples de stratégie d'autorisation dans la rubrique Exemples de politique d'identité.

Éléments de stratégie

Cette section décrit les éléments contenus dans les stratégies d'autorisation d'identité. Nous décrivons dans un premier temps les éléments à l'échelle de la stratégie, puis ceux qui s'appliquent uniquement à l'instruction dans laquelle ils sont inclus. Nous poursuivons avec une présentation sur la façon d'ajouter des conditions à vos instructions.

Pour obtenir des informations spécifiques sur la syntaxe des éléments, consultez Syntaxe du langage de stratégie IAM dans le Guide de l'utilisateur IAM.

Informations à l'échelle de la stratégie

Il existe deux éléments à l'échelle de la stratégie : `Id` et `Version`. Le tableau suivant fournit des informations sur ces éléments.

Name (Nom)	Description	Obligatoire	Valeurs valides
`Id`	Identifie la stratégie de façon unique.	Non	Toute chaîne
`Version`	Spécifie la version du langage d'accès aux stratégies.	Non	Toute chaîne. À titre de bonne pratique, nous vous recommandons d'inclure ce champ avec la valeur « 2012-10-17 ».

Déclarations propres à la stratégie

Les stratégies d'autorisation d'identité nécessitent au moins une instruction. Chaque instruction peut inclure les éléments décrits dans le tableau suivant.

Name (Nom)	Description	Obligatoire	Valeurs valides
`Sid`	Identifie l'instruction de façon unique.	Non	Toute chaîne.
`Effect`	Indique le résultat que vous voulez que l'instruction de la stratégie renvoie au moment de l'évaluation.	Oui	« Allow » ou « Deny ».
`Resource`	Indique l'identité à laquelle la stratégie s'applique. (Pour l'autorisation d'envoi, il s'agit de l'e-mail ou du domaine que le propriétaire de l'identité autorise l'expéditeur délégué à utiliser).	Oui	Amazon Resource Name (ARN) de l'identité.
`Principal`	Indique le Compte AWS, l'utilisateur ou le service AWS qui reçoit l'autorisation dans l'instruction.	Oui	ID Compte AWS valide, ARN de l'utilisateur ou service AWS. Compte AWS Les ID et les ARN des utilisateurs sont spécifiés en utilisant `"AWS"` (par exemple, `"AWS": ["1234567`

Name (Nom)	Description	Obligatoire	Valeurs valides
			`89012"]` ou `"AWS": ["arn:aws:iam::123456789012:root"]`). Les noms de service AWS sont spécifiés en utilisant `"Service"` (par exemple, `"Service": ["cognito-idp.amazonaws.com"]`). Pour obtenir des exemples du format des ARN utilisateur, consultez Références générales AWS.

Name (Nom)	Description	Obligatoire	Valeurs valides
`Action`	Indique l'action à laquelle s'applique l'instruction.	Oui	"ses:BatchGetMetricData", "ses:CancelExportJob", "ses:CreateDeliverabilityTestReport", "ses:CreateEmailIdentityPolicy", "ses:CreateExportJob", "ses:DeleteEmailIdentity", "ses:DeleteEmailIdentityPolicy", "ses:GetDomainStatisticsReport", "ses:GetEmailIdentity","ses:GetEmailIdentityPolicies", "ses:GetExportJob", "ses:ListExportJobs", "ses:ListRecommendations", "ses:PutEmailIdentityConfigurationSetAttributes", "ses:PutEmailIdentityDkimAttributes", "ses:PutEmailIdentityDkimSigningAttributes", "ses:PutEmailIdentityFeedbackAttributes", "ses:PutEmailIdentityMailFromAttributes", "ses:TagResource",

Name (Nom)	Description	Obligatoire	Valeurs valides
			"ses:UntagResource", "ses:UpdateEmailIdentityPolicy" (Actions d'autorisation d'envoi : "ses:SendEmail", "ses:SendRawEmail", "ses:SendTemplatedEmail", "ses:SendBulkTemplatedEmail") Vous pouvez spécifier une ou plusieurs de ces opérations.
`Condition`	Indique les restrictions éventuelles ou des détails sur l'autorisation.	Non	Consultez les informations sur les conditions à la suite de ce tableau.

Conditions

Une condition est une restriction qui s'applique à l'autorisation contenue dans l'instruction. La partie de l'instruction qui spécifie les conditions peut être la plus détaillée. Une clé est une caractéristique spécifique qui constitue la base pour une restriction d'accès (par exemple, la date et l'heure de la demande).

Vous utilisez à la fois les conditions et les clés afin d'exprimer la restriction. Par exemple, si vous voulez empêcher l'expéditeur délégué d'effectuer des demandes à Amazon SES en votre nom après le 30 juillet 2019, vous devez utiliser la condition appelée `DateLessThan`. Vous utilisez la clé appelée `aws:CurrentTime` et la définissez sur la valeur `2019-07-30T00:00:00Z`.

SES implémente uniquement les clés de stratégie à l'échelle AWS suivantes :

- `aws:CurrentTime`
- `aws:EpochTime`

- `aws:SecureTransport`
- `aws:SourceIp`
- `aws:SourceVpc`
- `aws:SourceVpce`
- `aws:UserAgent`
- `aws:VpcSourceIp`

Pour en savoir plus sur ces clés, consultez le guide de l'utilisateur IAM.

Exigences des stratégies

Les stratégies doivent répondre à toutes les exigences suivantes :

- Chaque stratégie doit inclure au moins une instruction.
- Chaque stratégie doit inclure au moins un mandataire valide.
- Chaque stratégie doit spécifier une ressource, et cette ressource doit être l'ARN de l'identité à laquelle la stratégie est attachée.
- Les propriétaires d'identité peuvent associer jusqu'à 20 stratégies à chaque identité.
- La taille d'une stratégie ne doit pas dépasser 4 kilo-octets (Ko).
- Le nom d'une stratégie ne doit pas dépasser 64 caractères. De plus, il ne peut inclure que des caractères alphanumériques, des tirets et des traits de soulignement.

Création d'une stratégie d'autorisation d'identité dans Amazon SES

Une stratégie d'autorisation d'identité est composée de déclarations spécifiant quelles actions API sont autorisées ou refusées pour une identité et sous quelles conditions.

Pour autoriser une identité de domaine ou d'adresse e-mail Amazon SES que vous possédez, vous créez une stratégie d'autorisation, puis vous attachez cette politique à l'identité. Une identité peut avoir zéro, une ou plusieurs stratégies. Toutefois, une stratégie ne peut être associée qu'à une seule identité.

Pour obtenir une liste des actions API pouvant être utilisées dans une stratégie d'autorisation d'identité, consultez la ligne Action du tableau the section called “Déclarations propres à la stratégie”.

Vous pouvez créer une stratégie d'autorisation d'identité de différentes manières :

- En utilisant le générateur de stratégies : vous pouvez créer une stratégie simple à l'aide du générateur de stratégies de la console SES. En plus d'autoriser ou de refuser les autorisations sur les actions de l'API SES, vous pouvez limiter les actions avec des conditions. Vous pouvez également utiliser le générateur de stratégies pour créer rapidement la structure de base d'une stratégie, puis la personnaliser ultérieurement en modifiant la stratégie.
- En créant une stratégie personnalisée : si vous souhaitez inclure des conditions plus avancées ou utiliser un service AWS comme principal, vous pouvez créer une stratégie personnalisée et l'attacher à l'identité à l'aide de la console SES ou de l'API SES.

Rubriques

Utilisation du Générateur de stratégies

Vous pouvez utiliser le générateur de politique pour créer une politique d'autorisation simple en suivant la procédure ci-dessous.

Pour créer une stratégie à l'aide du Générateur de stratégies

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).
3. Dans le conteneur Identities (Identités) de l'écran Verified identities (Identités vérifiées), sélectionnez l'identité vérifiée pour laquelle vous souhaitez créer une stratégie d'autorisation.
4. Dans l'écran des détails de l'identité vérifiée que vous avez sélectionnée à l'étape précédente, choisissez l'onglet Authorization (Autorisation).
5. Dans le panneau Authorization policies (Stratégies d'autorisation), choisissez Create policy (Créer une stratégie), puis sélectionnez Use policy generator (Utiliser le générateur de stratégie) depuis le menu déroulant.
6. Dans le panneau Create statement (Créer une instruction), choisissez Allow (Autoriser) dans le champ Effect (Effet). [Si vous voulez créer une stratégie pour restreindre cette identité, choisissez plutôt Deny (Refuser)].

7. Dans le champ Principals (Principaux), saisissez l'ID Compte AWS, l'ARN de l'utilisateur IAM ou le service AWS auquel sont attribuées les autorisations que vous souhaitez accorder pour cette identité, puis cliquez sur Add (Ajouter). (Si vous souhaitez en autoriser plus d'un, répétez cette étape pour chacun d'eux).
8. Dans le champ Actions, cochez la case de chaque action que vous souhaitez autoriser pour vos principaux.
9. (Facultatif) Développez Specify conditions (Spécifier les conditions) si vous souhaitez ajouter une instruction qualificative à l'autorisation.
    a. Sélectionnez un opérateur dans la liste déroulante Operator (Opérateur).
    b. Sélectionnez un type dans la liste déroulante Key (Clé).
    c. En fonction du type de clé que vous avez sélectionné, saisissez sa valeur dans le champ Value (Valeur). (Si vous souhaitez ajouter d'autres conditions, choisissez Add new condition (Ajouter une nouvelle condition) et répétez cette étape pour chaque condition supplémentaire.)
10. Choisissez Save statement (Enregistrer l'instruction).
11. (Facultatif) Développez Create another statement (Créer une autre instruction) si vous souhaitez ajouter d'autres instructions à votre politique et répétez les étapes 6 à 10.
12. Choisissez Next (Suivant) et sur l'écran Customize policy (Personnaliser la politique), le conteneur Edit policy details (Modifier les détails de la politique) contient des champs où vous pouvez modifier ou personnaliser le Name (Nom) de la politique et le Policy document (Document de la politique) proprement dit.
13. Choisissez Next (Suivant) et sur l'écran Review and apply (Vérifier et appliquer), le conteneur Overview (Présentation) affiche l'identité vérifiée que vous autorisez ainsi que le nom de cette stratégie. Dans le panneau Policy document (Document de politique), vous trouverez la politique que vous venez de rédiger ainsi que toutes les conditions que vous avez ajoutées ; vérifiez la politique et si elle semble correcte, choisissez Apply policy (Appliquer la stratégie). (Si vous avez besoin de modifier ou corriger quelque chose, choisissez Previous (Précédent) et travaillez dans le conteneur Edit policy details (Modification des détails de la politique).)

Création d'une stratégie personnalisée

Si vous souhaitez créer une stratégie personnalisée et l'attacher à une identité, voici les possibilités qui s'offrent à vous :

- Utilisation de l'API Amazon SES – Créez une stratégie dans un éditeur de texte, puis attachez-la à l'identité à l'aide de l'API `PutIdentityPolicy` décrite dans le document Référence d'API Amazon Simple Email Service.
- Utilisation de la console Amazon SES – Créez une stratégie dans un éditeur de texte et attachez-la à une identité en la collant dans l'éditeur de stratégie personnalisée de la console Amazon SES. La procédure suivante décrit cette méthode.

Pour créer une stratégie personnalisée à l'aide de l'éditeur de stratégie personnalisée

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).
3. Dans le conteneur Identities (Identités) de l'écran Verified identities (Identités vérifiées), sélectionnez l'identité vérifiée pour laquelle vous souhaitez créer une stratégie d'autorisation.
4. Dans l'écran des détails de l'identité vérifiée que vous avez sélectionnée à l'étape précédente, choisissez l'onglet Authorization (Autorisation).
5. Dans le panneau Authorization policies (Stratégies d'autorisation), choisissez Create policy (Créer une stratégie), puis sélectionnez Create custom policy (Créer une stratégie personnalisée) depuis le menu déroulant.
6. Dans le volet Policy document (Document de la stratégie), saisissez ou collez le texte de votre stratégie au format JSON. Vous pouvez également utiliser le générateur de stratégies pour créer rapidement la structure de base d'une stratégie, puis la personnaliser ici.
7. Choisissez Apply Policy (Appliquer la stratégie). (Si vous avez besoin de modifier votre politique personnalisée, il suffit de cocher sa case à cocher sous l'onglet Authorization (Autorisation), choisir Edit (Modifier), et effectuer vos modifications dans le panneau Document de politique pour finir par Save changes (Enregistrer les modifications)).

Exemples de politiques d'identité dans Amazon SES

L'autorisation de l'identité vous permet de spécifier les conditions précises dans lesquelles vous autorisez ou refusez les actions de l'API pour une identité.

Les exemples suivants vous montrent comment écrire des stratégies pour contrôler différents aspects des actions de l'API :

- Spécifier le principal
- Restriction de l'action
- Utilisation de plusieurs instructions

Spécifier le principal

Le principal, c'est-à-dire l'entité à laquelle vous accordez des autorisations, peut être un Compte AWS, un utilisateur AWS Identity and Access Management (IAM) ou un service AWS appartenant au même compte.

L'exemple suivant montre une stratégie simple qui permet à l'ID AWS 123456789012 de contrôler l'identité vérifiée exemple.com, qui est également détenue par le Compte AWS 123456789012.

```
{
  "Id":"SampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeMarketer",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:123456789012:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
      "Action":[
        "ses:DeleteEmailIdentity",
        "ses:PutEmailIdentityDkimSigningAttributes"
      ]
    }
  ]
}
```

L'exemple de stratégie suivant accorde des autorisations à deux utilisateurs pour contrôler l'identité vérifiée example.com. Les utilisateurs sont spécifiés par leur Amazon Resource Name (ARN).

```
{
  "Id":"ExampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
```

```
    {
      "Sid":"AuthorizeIAMUser",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:123456789012:identity/example.com",
      "Principal":{
        "AWS":[
          "arn:aws:iam::123456789012:user/John",
          "arn:aws:iam::123456789012:user/Jane"
        ]
      },
      "Action":[
        "ses:DeleteEmailIdentity",
        "ses:PutEmailIdentityDkimSigningAttributes"
      ]
    }
  ]
}
```

Restriction de l'action

Il existe plusieurs actions qui peuvent être spécifiées dans une stratégie d'autorisation d'identité en fonction du niveau de contrôle que vous souhaitez autoriser :

```
"BatchGetMetricData",
"ListRecommendations",
"CreateDeliverabilityTestReport",
"CreateEmailIdentityPolicy",
"DeleteEmailIdentity",
"DeleteEmailIdentityPolicy",
"GetDomainStatisticsReport",
"GetEmailIdentity",
"GetEmailIdentityPolicies",
"PutEmailIdentityConfigurationSetAttributes",
"PutEmailIdentityDkimAttributes",
"PutEmailIdentityDkimSigningAttributes",
"PutEmailIdentityFeedbackAttributes",
"PutEmailIdentityMailFromAttributes",
"TagResource",
"UntagResource",
"UpdateEmailIdentityPolicy"
```

Les stratégies d'autorisation d'identité vous permettent également de restreindre le principal à une seule de ces actions.

```
{
  "Id":"ExamplePolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"ControlAction",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:123456789012:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
      "Action":[
        "ses:PutEmailIdentityMailFromAttributes
      ]
    }
  ]
}
```

Utilisation de plusieurs instructions

Votre stratégie d'autorisation d'identité peut inclure plusieurs instructions. L'exemple de stratégie suivant comporte deux instructions. La première déclaration interdit à deux utilisateurs d'accéder à `getemailidentity` à partir de sender@example.com au sein du même compte `123456789012`. La deuxième déclaration refuse l'accès à `UpdateEmailIdentityPolicy` au principal, Jack, dans le même compte `123456789012`.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"DenyGet",
      "Effect":"Deny",
      "Resource":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
      "Principal":{
        "AWS":[
          "arn:aws:iam::123456789012:user/John",
          "arn:aws:iam::123456789012:user/Jane"
        ]
      },
      "Action":[
```

```
        "ses:GetEmailIdentity"
      ]
    },
    {
      "Sid":"DenyUpdate",
      "Effect":"Deny",
      "Resource":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
      "Principal":{
        "AWS":"arn:aws:iam::123456789012:user/Jack"
      },
      "Action":[
        "ses:UpdateEmailIdentityPolicy"
      ]
    }
  ]
}
```

Gestion de vos stratégies d'autorisation d'identité dans Amazon SES

En plus de créer des stratégies et de les attacher à des identités, vous pouvez modifier, supprimer, répertorier et récupérer les stratégies d'une identité, comme indiqué dans les sections suivantes.

Gestion des stratégies à l'aide de la console Amazon SES

La gestion des politiques Amazon SES implique d'afficher, de modifier ou de supprimer une politique attachée à une identité à l'aide de la console Amazon SES.

Pour gérer les politiques à l'aide de la console Amazon SES

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).
3. Dans la liste des identités, choisissez l'identité que vous souhaitez gérer.
4. Sur la page de détails de l'identité, accédez à l'onglet Authorization (Autorisation). Vous trouverez ici une liste de toutes les stratégies attachées à cette identité.
5. Sélectionnez la politique que vous souhaitez gérer en cochant sa case à cocher.
6. En fonction de la tâche de gestion souhaitée, choisissez le bouton correspondant comme suit :

a. Pour afficher la politique, choisissez View policy (Afficher la politique). Si vous avez besoin d'une copie de ce document, cliquez sur le bouton Copy (Copier) et il sera copié dans votre presse-papiers.

b. Pour modifier la politique, choisissez Edit (Modifier). Dans le panneau Policy document (Document de politique), modifiez la politique, puis choisissez Save changes (Enregistrer les modifications).

> **Note**
>
> Pour révoquer des autorisations, vous pouvez soit modifier une stratégie, soit la supprimer.

c. Pour supprimer la politique, choisissez Delete (Supprimer).

> **Important**
>
> La suppression d'une stratégie est permanente. Avant de supprimer une stratégie, nous vous recommandons de la sauvegarder en la copiant-collant dans un fichier texte.

Gestion des stratégies à l'aide de l'API Amazon SES

La gestion des politiques Amazon SES implique d'afficher, de modifier ou de supprimer une politique attachée à une identité à l'aide de l'API Amazon SES.

Pour répertorier et afficher des stratégies à l'aide de l'API Amazon SES

- Vous pouvez répertorier les stratégies attachées à une identité à l'aide de l'opération d'API ListIdentityPolicies. Vous pouvez également extraire les stratégies proprement dites à l'aide de l'opération d'API GetIdentityPolicies.

Pour modifier une politique à l'aide de l'API Amazon SES

- Vous pouvez modifier une politique attachée à une identité à l'aide de l'opération d'API PutIdentityPolicy.

Pour supprimer une politique à l'aide de l'API Amazon SES

- Vous pouvez supprimer une politique attachée à une identité à l'aide de l'opération d'API DeleteIdentityPolicy.

Utilisation de l'autorisation d'envoi avec Amazon SES

Vous pouvez configurer Amazon SES pour autoriser d'autres utilisateurs à envoyer des e-mails à partir des identités que vous possédez (domaines ou adresses e-mail) en utilisant leurs propres comptes Amazon SES. Grâce à la fonction d'autorisation d'envoi, vous pouvez garder le contrôle de vos identités pour pouvoir modifier ou révoquer les autorisations à tout moment. Par exemple, si vous êtes propriétaire d'une entreprise, vous pouvez utiliser l'autorisation d'envoi pour permettre à un tiers (une société de marketing par e-mail, par exemple) d'envoyer des e-mails à partir d'un domaine que vous possédez.

Ce chapitre couvre les spécificités de l'autorisation d'envoi qui remplace l'ancienne fonction de notifications inter-comptes. Vous devez d'abord comprendre les bases de l'autorisation basée sur l'identité à l'aide de stratégies d'autorisation, comme expliqué dans le document Utilisation de l'autorisation d'identité dans Amazon SES, qui couvre des sujets importants tels que l'anatomie d'une stratégie d'autorisation et la façon de gérer vos stratégies.

Prise en charge de l'héritage des notifications entre comptes

Les notifications de commentaires pour les retours à l'expéditeur, les réclamations et les remises associées aux e-mails envoyés par un expéditeur délégué qui a été autorisé par un propriétaire d'identité à envoyer à partir d'une de ses identités vérifiées, ont traditionnellement été configurées à l'aide de notifications entre comptes où l'expéditeur délégué associerait une rubrique avec une identité dont il n’est pas propriétaire (c'est-à-dire le compte croisé). Toutefois, les notifications entre comptes ont été remplacées par l'utilisation de jeux de configuration et d'identités vérifiées, combinée à l'envoi délégué pour lequel l'expéditeur délégué a été autorisé par le propriétaire de l'identité à utiliser l'une de ses identités vérifiées pour envoyer des e-mails. Cette nouvelle méthode donne la flexibilité nécessaire pour configurer les notifications de retour à l'expéditeur, de réclamation, de remise et d'autres événements par les deux constructions suivantes selon que vous êtes l'expéditeur délégué ou le propriétaire de l'identité vérifiée :

- Jeux de configurations – L'expéditeur délégué peut configurer la publication d'événements dans son propre jeu de configurations qu'il peut spécifier lors de l'envoi d'un e-mail à partir d'une identité vérifiée dont il n'est pas propriétaire, mais qu'il a été autorisé à envoyer par le propriétaire de

l'identité via une politique d'autorisation. La publication d'événements permet de publier des notifications de rebond, de plainte, de livraison et d'autres événements sur Amazon CloudWatch, Amazon Data Firehose, Amazon Pinpoint et Amazon SNS. veuillez consulter Créer des destination d'évenement.

- Identités vérifiées – Outre que le propriétaire de l'identité autorise l'expéditeur délégué à utiliser l'une de ses identités vérifiées pour envoyer des e-mails, il peut également, à la demande de l'expéditeur délégué, configurer des notifications de commentaires sur l'identité partagée pour utiliser les rubriques SNS appartenant à l'expéditeur délégué. Seul l'expéditeur délégué recevra ces notifications, car il est propriétaire de la rubrique SNS. Voir l'étape 14 pour savoir comment configurer une « rubrique SNS que vous ne possédez pas » dans les procédures de politique d'autorisation.

> **Note**
>
> Pour des raisons de compatibilité, les notifications entre comptes sont prises en charge pour les notifications entre comptes héritées actuellement utilisées dans votre compte. Cette prise en charge se limite à la possibilité de modifier et d'utiliser tous les comptes croisés que vous avez créés dans la console classique Amazon SES. Toutefois, vous ne pouvez plus créer de nouvelles notifications entre comptes. Pour en créer de nouvelles dans la nouvelle console Amazon SES, utilisez les nouvelles méthodes d'envoi délégué avec des jeux de configurations utilisant publication d'événement, ou avec des identités vérifiées configurées avec vos propres rubriques SNS.

Rubriques

Présentation de l'autorisation d'envoi Amazon SES

Cette rubrique offre une présentation du processus d'autorisation d'envoi et explique comment les fonctions d'envoi d'e-mails d'Amazon SES, telles que les quotas d'envoi et les notifications, fonctionnent avec l'autorisation d'envoi.

Cette section utilise les termes suivants :

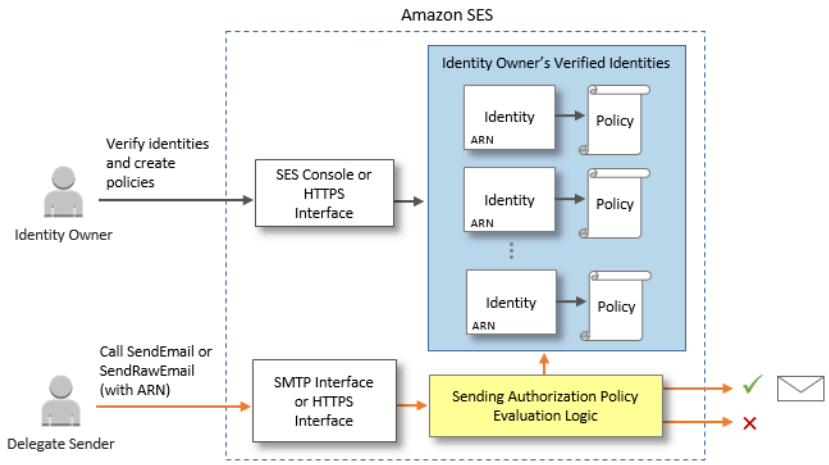
- Identité – Adresse e-mail ou domaine dont se servent les utilisateurs Amazon SES pour envoyer un e-mail.
- Propriétaire d'identité – Utilisateur Amazon SES dont la propriété d'une adresse e-mail ou d'un domaine a été vérifiée selon les procédures décrites dans Identités vérifiées.
- Expéditeur délégué – Un compte AWS, un utilisateur AWS Identity and Access Management (IAM), ou un service AWS autorisé par le biais d'une politique d'autorisation pour envoyer des e-mails au nom du propriétaire de l'identité.
- Stratégie d'autorisation d'envoi – Document que vous attachez à une identité pour spécifier les personnes habilitées à effectuer des envois pour cette identité et sous quelles conditions.
- ARN (Amazon Resource Name) – Moyen standardisé d'identifier de manière unique une ressource AWS à travers tous les services AWS. Pour l'autorisation d'envoi, la ressource est l'identité que le propriétaire de l'identité veut que l'expéditeur délégué utilise. Voici un exemple d'ARN : arn:aws:ses:us-east-1:123456789012:identity/example.com.

Processus d'autorisation d'envoi

L'autorisation d'envoi repose sur des stratégies d'autorisation d'envoi. Si vous souhaitez permettre à un expéditeur délégué d'effectuer un envoi en votre nom, vous devez créer une stratégie d'autorisation d'envoi et l'associer à votre identité à l'aide de la console Amazon SES ou de l'API Amazon SES. Lorsque l'expéditeur délégué tente d'envoyer un e-mail via Amazon SES en votre nom, il transmet l'ARN de votre identité dans la demande ou dans l'en-tête de l'e-mail.

Lorsqu'Amazon SES reçoit la demande d'envoi de l'e-mail et qu'une stratégie existe pour votre identité, cette dernière est vérifiée pour déterminer si vous avez autorisé l'expéditeur délégué à effectuer un envoi au nom de l'identité. Si l'expéditeur délégué est autorisé, Amazon SES accepte l'e-mail ; dans le cas contraire, Amazon SES renvoie un message d'erreur.

Le schéma suivant illustre la relation globale entre les concepts d'autorisation d'envoi :



Le processus d'autorisation d'envoi se compose des trois étapes suivantes :

1. Le propriétaire d'identité sélectionne une identité vérifiée que l'expéditeur délégué doit utiliser. (Si vous n'avez pas vérifié d'identité, consultez Identités vérifiées.)

   > **Note**
   >
   > Aucun jeu de configurations par défaut ne doit être affecté à l'identité vérifiée que vous choisissez pour votre expéditeur délégué.

2. L'expéditeur délégué fait savoir au propriétaire de l'identité quel ID de compte AWS ou ARN d'utilisateur IAM il souhaite utiliser pour l'envoi.
3. Si le propriétaire de l'identité accepte d'autoriser l'expéditeur délégué à effectuer des envois à partir de l'un des comptes du propriétaire, celui-ci crée une politique d'autorisation d'envoi et l'attache à l'identité choisie en utilisant la console Amazon SES ou l'API Amazon SES.
4. Le propriétaire de l'identité donne à l'expéditeur délégué l'ARN de l'identité autorisée afin que l'expéditeur délégué puisse fournir l'ARN à Amazon SES au moment de l'envoi de l'e-mail.
5. L'expéditeur délégué peut configurer des notifications de retour à l'expéditeur et de réclamation via la publication d'événement activée dans un jeu de configurations spécifié lors de l'envoi délégué. Le propriétaire de l'identité peut également configurer des notifications de commentaires par e-mail pour les événements de retour à l'expéditeur et de réclamation à envoyer aux rubriques Amazon SNS de l'expéditeur délégué.

> **Note**
>
> Si le propriétaire de l'identité désactive l'envoi de notifications d'événements, l'expéditeur délégué doit configurer la publication d'événements pour publier les événements de rebond et de plainte sur une rubrique Amazon SNS ou un stream Firehose. L'expéditeur doit également appliquer le jeu de configurations qui contient la règle de publication d'événements à chaque e-mail qu'il envoie. Si ni le propriétaire d'identité ni l'expéditeur délégué ne configure une méthode d'envoi de notifications d'événements de retour à l'expéditeur et de réclamation, ou si l'expéditeur n'applique pas le jeu de configurations qui utilise la règle de publication d'événements, Amazon SES envoie automatiquement les notifications d'événements par e-mail à l'adresse indiquée dans le champ Return-Path (Chemin de retour) de l'e-mail (ou à l'adresse du champ Source si vous n'avez pas spécifié d'adresse Return-Path (Chemin de retour)), même si le propriétaire d'identité a désactivé le transfert de commentaires par e-mail.

6. L'expéditeur délégué tente d'envoyer un e-mail via Amazon SES au nom du propriétaire d'identité en transmettant l'ARN de l'identité de son propriétaire dans la demande ou dans l'en-tête de l'e-mail. L'expéditeur délégué peut envoyer l'e-mail à partir de l'interface SMTP Amazon SES ou de l'API Amazon SES. À réception de la demande, Amazon SES examine les stratégies éventuellement attachées à l'identité et accepte l'e-mail si l'expéditeur délégué est autorisé à utiliser les adresses d'expédition et de chemin de retour spécifiées ; sinon, Amazon SES renvoie une erreur et n'accepte pas le message.

   > **Important**
   >
   > Le compte AWS de l'expéditeur délégué doit être supprimé de l'environnement de test (sandbox) pour que l'envoi d'e-mails soit utilisé afin d'envoyer des e-mails à des adresses non vérifiées.

7. Si le propriétaire d'identité doit annuler l'autorisation accordée à l'expéditeur délégué, il modifie simplement la stratégie d'autorisation d'envoi ou la supprime entièrement. Le propriétaire d'identité peut effectuer l'une ou l'autre de ces actions à l'aide de la console Amazon SES ou de l'API Amazon SES.

Pour en savoir plus sur la façon dont le propriétaire d'identité ou l'expéditeur délégué effectue ces tâches, consultez respectivement Tâches de propriétaire d'identité ou Tâches d'expéditeur délégué.

Attribution des fonctions d'envoi d'e-mail

Il est important de comprendre le rôle de l'expéditeur délégué et du propriétaire d'identité par rapport aux fonctions d'envoi de courrier électronique Amazon SES, telles que le quota d'envoi quotidien, les retours à l'expéditeur et les réclamations, la signature DKIM, le transfert de commentaires, etc. L'attribution est la suivante :

- Quotas d'envoi – Les e-mails envoyés à partir d'identités de propriétaire d'identité sont comptabilisés par rapport au quota de l'expéditeur délégué.
- Retours à l'expéditeur et réclamations – Les événements de retour à l'expéditeur et de réclamation sont enregistrés par rapport au compte Amazon SES de l'expéditeur délégué et peuvent donc influer sur la réputation de l'expéditeur délégué.
- Signature DKIM – Si le propriétaire d'identité a activé la signature Easy DKIM pour une identité, tous les e-mails envoyés à partir de cette identité sont signés par DKIM, y compris ceux envoyés par l'expéditeur délégué. Le propriétaire d'identité est le seul à pouvoir contrôler que les e-mails ont une signature DKIM.
- Notifications – Le propriétaire d'identité et l'expéditeur délégué peuvent configurer des notifications de retours à l'expéditeur et de réclamations. Le propriétaire d'identité des e-mails peut aussi activer le transfert de commentaires par e-mail. Pour en savoir plus sur la configuration des notifications, consultez Surveillance de votre activité d'envoi Amazon SES.
- Vérification – Les propriétaires d'identité sont tenus de suivre la procédure décrite dans Identités vérifiées pour vérifier qu'ils sont propriétaires des adresses e-mail et des domaines qu'ils autorisent les expéditeurs délégués à utiliser. Les expéditeurs délégués n'ont pas besoin de vérifier les adresses e-mail ou les domaines précisément pour l'autorisation d'envoi.

  > **Important**
  >
  > Le compte AWS de l'expéditeur délégué doit être supprimé de l'environnement de test (sandbox) pour que l'envoi d'e-mails soit utilisé afin d'envoyer des e-mails à des adresses non vérifiées.

- Régions AWS – L'expéditeur délégué doit envoyer les e-mails à partir de la région AWS dans laquelle l'identité de son propriétaire est vérifiée. La stratégie d'autorisation d'envoi qui donne l'autorisation à l'expéditeur délégué doit être attachée à l'identité de cette région.
- Facturation – Tous les messages envoyés à partir du compte de l'expéditeur délégué, y compris les e-mails que l'expéditeur délégué envoie à l'aide des adresses du propriétaire d'identité, sont facturés à l'expéditeur délégué.

Tâches de propriétaire d'identité pour l'autorisation d'envoi Amazon SES

Cette section décrit les étapes que les propriétaires d'identité doivent effectuer lors de la configuration d'une autorisation d'envoi.

Rubriques

Vérification d'une identité pour l'autorisation d'envoi Amazon SES

La première étape de configuration de l'autorisation d'envoi consiste à prouver que vous êtes le propriétaire de l'adresse e-mail ou du domaine à partir duquel l'expéditeur délégué enverra des e-mails. La procédure de vérification est décrite dans Identités vérifiées.

Vous pouvez confirmer qu'une adresse e-mail ou un domaine a été contrôlé en vérifiant son statut dans la section Gestion des identités de https://console.aws.amazon.com/ses/ ou en utilisant l'opération d'API `GetIdentityVerificationAttributes`.

Avant que vous ou l'expéditeur délégué puissiez envoyer des e-mails à des adresses e-mail non vérifiées, vous devez soumettre une demande pour que votre compte soit supprimé de l'environnement de test (sandbox) Amazon SES. Pour plus d'informations, consultez Demande d'accès à la production (sortie du sandbox d'Amazon SES).

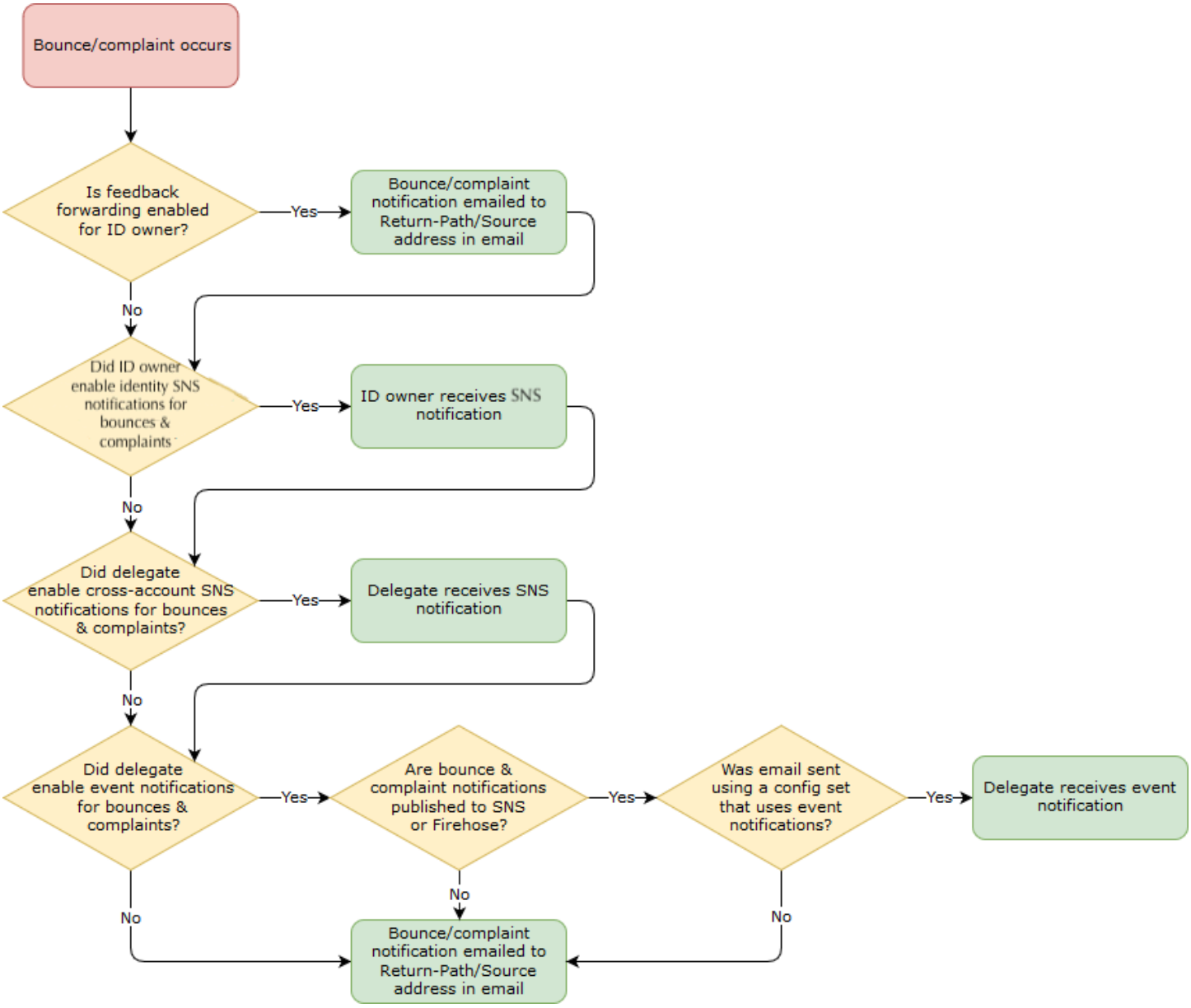
> **Important**
>
> Le Compte AWS de l'expéditeur délégué doit être supprimé de l'analyseur de contrôle (sandbox) pour que l'envoi d'e-mails soit utilisé afin d'envoyer des e-mails à des adresses non vérifiées.

Configuration des notifications du propriétaire d'identité pour l'autorisation d'envoi Amazon SES

Si vous autorisez un expéditeur délégué à envoyer des e-mails en votre nom, Amazon SES comptabilise tous les retours à l'expéditeur et les réclamations générés par ces e-mails dans les métriques de retours à l'expéditeur et de réclamations de l'expéditeur délégué et non dans les vôtres. Toutefois, si vos adresses IP apparaissent sur des anti-spam tiers, des listes de trous noirs basées sur le DNS (DNS-based Blackhole Lists, ou DNSBL), à la suite de messages envoyés par un expéditeur délégué, la réputation de vos identités risque d'être affectée. C'est pourquoi, si vous êtes propriétaire d'une identité, vous devez configurer le transfert des retours d'e-mail pour toutes vos identités, y compris celles que vous avez autorisées pour l'envoi délégué. Pour plus d'informations, consultez Réception des notifications Amazon SES par e-mail.

Les expéditeurs délégués peuvent et doivent configurer leurs propres notifications de retour à l'expéditeur et de réclamation pour les identités que vous les avez autorisés à utiliser. Ils peuvent configurer la publication d'événements pour publier les événements de rebond et de plainte sur une rubrique Amazon SNS ou un stream Firehose.

Si ni le propriétaire d'identité ni l'expéditeur délégué ne configure une méthode d'envoi de notifications d'événements de retour à l'expéditeur et de réclamation, ou si l'expéditeur n'applique pas le jeu de configurations qui utilise la règle de publication d'événements, Amazon SES envoie automatiquement les notifications d'événements par e-mail à l'adresse indiquée dans le champ Return-Path (Chemin de retour) de l'e-mail (ou à l'adresse du champ Source si vous n'avez pas spécifié d'adresse Return-Path (Chemin de retour)), même si vous avez désactivé le transfert de commentaires par e-mail. Ce processus est illustré à l'image suivante.



Obtention d'informations auprès de l'expéditeur délégué pour l'autorisation d'envoi Amazon SES

Votre politique d'autorisation d'envoi doit spécifier au moins un principal, qui est l'entité de votre expéditeur délégué à laquelle vous accordez l'accès afin qu'il puisse effectuer des envois au nom de l'une de vos identités vérifiées. Pour les politiques d'autorisation d'envoi Amazon SES, le principal peut être le compte AWS de votre expéditeur délégué, un ARN utilisateur AWS Identity and Access Management (IAM) ou un service AWS.

Une manière facile d'y penser est que le principal(expéditeur délégué) est le bénéficiaire, et vous (propriétaire de l'identité) êtes le concédant dans la politique d'autorisation dans laquelle vous lui

accordez l'autorisation d'envoyer n'importe quelle combinaison d'e-mails, d'e-mails bruts, de modèles d'e-mails ou modèles d'e-mails groupés à partir de la ressource (identité vérifiée) que vous possédez.

Si vous souhaitez un contrôle plus précis, demandez à l'expéditeur délégué de configurer un utilisateur IAM afin qu'un seul expéditeur délégué puisse envoyer pour vous plutôt que n'importe quel utilisateur du compte AWS de l'expéditeur délégué. L'expéditeur délégué peut trouver des informations sur la configuration d'un utilisateur IAM dans la section Création d'un utilisateur IAM dans votre compte AWS dans le Guide de l'utilisateur IAM.

Demandez à votre expéditeur délégué l'ID du compte AWS ou l'Amazon Resource Name (ARN) de l'utilisateur IAM afin de l'inclure dans votre politique d'autorisation d'envoi. Vous pouvez renvoyer l'expéditeur délégué aux instructions permettant de trouver ces informations dans Communication d'informations au propriétaire d'identité. Si l'expéditeur délégué est un service AWS, consultez la documentation correspondante pour déterminer le nom du service.

L'exemple de politique suivant illustre les éléments de base de ce qui est nécessaire dans une politique créée par le propriétaire de l'identité pour autoriser l'expéditeur délégué à envoyer depuis la ressource du propriétaire de l'identité. Le propriétaire de l'identité se rendrait dans le flux des identités vérifiées et, sous la rubrique autorisation, utiliserait le générateur de politiques pour créer, dans sa forme la plus simple, la politique de base suivante autorisant l'expéditeur délégué à envoyer au nom d'une ressource appartenant au propriétaire de l'identité :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "stmt1632010098378",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "ses:SendEmail",
                "ses:SendRawEmail"
            ],
            "Resource": "arn:aws:ses:us-east-1:444455556666:identity/bob@example.com",
            "Condition": {}
        }
    ]
}
```

Pour la politique ci-dessus, la légende suivante explique les éléments clés et à qui ils appartiennent :

- Principal : ce champ est renseigné avec l'ARN utilisateur IAM de l'expéditeur délégué.
- Action : ce champ contient deux actions SES (`SendEmail` & `SendRawEmail`) que le propriétaire de l'identité autorise l'expéditeur délégué à effectuer à partir de la ressource du propriétaire de l'identité.
- Ressource : ce champ contient la ressource vérifiée du propriétaire de l'identité à partir de laquelle il autorise l'expéditeur délégué à envoyer.

Création d'une stratégie pour l'autorisation d'envoi Amazon SES

Comme pour la création de toute politique d'autorisation dans Amazon SES, comme expliqué dans Création d'une stratégie d'autorisation d'identité, pour autoriser un expéditeur délégué à envoyer des e-mails en utilisant une adresse e-mail ou un domaine (une identité) que vous possédez, vous créez la stratégie en spécifiant les actions de l'API d'envoi SES, puis vous attachez cette stratégie à l'identité.

Pour obtenir une liste des actions API qui peuvent être spécifiées dans une stratégie pour l'autorisation d'envoi, consultez la ligne Action du tableau the section called “Déclarations propres à la stratégie”.

Vous pouvez créer une stratégie pour l'autorisation d'envoi en utilisant le générateur de stratégies ou en créant une stratégie personnalisée. Des procédures spécifiques à la création d'une stratégie pour l'autorisation d'envoi sont fournies pour l'une ou l'autre méthode.

> **Note**
>
> - Les stratégies d'autorisation d'envoi que vous attachez à des identités d'adresse e-mail ont priorité sur les stratégies que vous attachez à leur identité de domaine correspondante. Par exemple, si vous créez une politique pour example.com, qui interdit un expéditeur délégué, et créez une politique pour sender@example.com, qui autorise l'expéditeur délégué, l'expéditeur délégué peut envoyer des e-mails à partir de sender@example.com, mais pas à partir d'une autre adresse du domaine example.com.
> - Si vous créez une stratégie pour example.com qui autorise un expéditeur délégué, et que vous créez une stratégie pour sender@example.com qui interdit l'expéditeur délégué, l'expéditeur délégué peut envoyer des e-mails à partir de n'importe quelle adresse du domaine example.com à l'exception de sender@example.com.

- Si vous connaissez mal la structure des mécanismes d'autorisation de SES, consultez Structure de la stratégie.

Création d'une stratégie pour l'autorisation d'envoi à l'aide d'un générateur de stratégies.

Vous pouvez utiliser le générateur de stratégie pour créer une stratégie pour l'autorisation d'envoi en suivant la procédure ci-dessous.

Pour créer une stratégie pour l'autorisation d'envoi en utilisant le générateur de stratégie

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES sur la page https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).
3. Dans le conteneur Identities (Identités) sur l'écran Verified identities (Identités vérifiées), sélectionnez l'identité vérifiée pour laquelle vous souhaitez autoriser l'expéditeur délégué à envoyer en votre nom.
4. Choisissez l'onglet Autorisation de l'identité vérifiée.
5. Dans le panneau Authorization policies (Stratégies d'autorisation), choisissez Create policy (Créer une stratégie), puis sélectionnez Use policy generator (Utiliser le générateur de stratégie) depuis le menu déroulant.
6. Dans le panneau Create statement (Créer une instruction), choisissez Allow (Autoriser) dans le champ Effect (Effet). (Si vous souhaitez créer une politique visant à restreindre votre expéditeur délégué, choisissez Deny (Refuser) à la place.)
7. Dans le champ Principals (Principal), entrez l'ID Compte AWS ou l'ARN de l'utilisateur IAM que votre expéditeur délégué a partagé avec vous pour l'autoriser à envoyer un e-mail au nom de votre compte pour cette identité, puis choisissez Add (Ajouter). (Si vous souhaitez autoriser plusieurs expéditeurs délégués, répétez cette étape pour chacun d'eux.)
8. Dans le champ Actions, cochez la case correspondant à chaque type d'envoi que vous souhaitez autoriser pour votre expéditeur délégué.
9. (Facultatif) Développez Specify conditions (Spécifiez les conditions) si vous souhaitez ajouter une instruction qualificative à l'autorisation de l'expéditeur délégué.
    a. Sélectionnez un opérateur dans la liste déroulante Operator (Opérateur).
    b. Sélectionnez un type dans la liste déroulante Key (Clé).

c. En fonction du type de clé que vous avez sélectionné, saisissez sa valeur dans le champ Value (Valeur). (Si vous souhaitez ajouter d'autres conditions, choisissez Add new condition (Ajouter une nouvelle condition) et répétez cette étape pour chaque condition supplémentaire.)

10. Choisissez Save statement (Enregistrer l'instruction).
11. (Facultatif) Développez Create another statement (Créer une autre instruction) si vous souhaitez ajouter d'autres instructions à votre politique et répétez les étapes 6 à 10.
12. Choisissez Next (Suivant) et sur l'écran Customize policy (Personnaliser la politique), le conteneur Edit policy details (Modifier les détails de la politique) contient des champs où vous pouvez modifier ou personnaliser le Name (Nom) de la politique et le Policy document (Document de la politique) proprement dit.
13. Choisissez Next (Suivant) et sur l'écran Review and apply (Vérifier et appliquer), le conteneur Overview (Présentation) affiche l'identité vérifiée que vous autorisez pour votre expéditeur délégué ainsi que le nom de cette politique. Dans le panneau Policy document (Document de politique), vous trouverez la politique que vous venez de rédiger ainsi que toutes les conditions que vous avez ajoutées ; vérifiez la politique et si elle semble correcte, choisissez Apply policy (Appliquer la stratégie). (Si vous avez besoin de modifier ou corriger quelque chose, choisissez Previous (Précédent) et travaillez dans le conteneur Edit policy details (Modification des détails de la politique).) La politique que vous venez de créer permettra à votre expéditeur délégué d'envoyer en votre nom.
14. (Facultatif) Si votre expéditeur délégué souhaite également utiliser une rubrique SNS dont il est propriétaire, pour recevoir des notifications de commentaires lorsqu'il reçoit des retours à l'expéditeur ou des réclamations, ou lorsque les e-mails sont délivrés, vous devrez configurer sa rubrique SNS dans cette identité vérifiée. (Votre expéditeur délégué devra partager avec vous son ARN de rubrique SNS.) Sélectionnez l'onglet Notifications et sélectionnezEdit (Modifier) dans le conteneur Feedback notifications (Notifications de commentaire) :

    a. Dans le panneau Configure SNS topics (Configuration des rubriques SNS(, l'un des champs de retour, (retour à l'expéditeur, réclamation ou remise), sélectionnez SNS topic you don't own (Sujet SNS que vous ne possédez pas) et saisissez le SNS topic ARN (ARN de rubrique SNS) détenu et partagé avec vous par votre expéditeur délégué. (Seul l'expéditeur délégué recevra ces notifications, car il est propriétaire de la rubrique SNS ; vous, en tant que propriétaire de l'identité, ne les recevrez pas.)
    b. (Facultatif) Si vous souhaitez que votre notification de rubrique inclue les en-têtes de l'e-mail d'origine, cochez la case Include original email headers (Incluez les en-têtes

d'e-mail d'origine) située directement sous le nom de rubrique SNS de chaque type de commentaires. Cette option est disponible uniquement si vous avez affecté une rubrique Amazon SNS au type de notification associé. Pour en savoir plus sur le contenu des en-têtes de l'e-mail d'origine, consultez l'objet `mail` dans Contenu des notifications .

c. Sélectionnez Save Changes (Enregistrer les modifications). L'application des modifications que vous apportez à vos paramètres de notification peut prendre quelques minutes.

d. (Facultatif) Étant donné que votre expéditeur délégué recevra des notifications de rubriques Amazon SNS pour les retours à l'expéditeur et les réclamations, vous pouvez désactiver entièrement les notifications par e-mail si vous ne souhaitez pas recevoir de commentaires concernant les envois de cette identité. Pour désactiver les commentaires par e-mail pour les retours à l'expéditeur et les réclamations, sous l'onglet Notifications, dans le conteneur Email Feedback Forwarding (Transfert de commentaires par e-mail), choisissez Edit (Modifier), décochez la case Enabled (Activé), et choisissez Save changes (Enregistrer les modifications). Les notifications de statut de livraison seront désormais envoyées uniquement aux rubriques SNS appartenant à votre expéditeur délégué.

Création d'une stratégie personnalisée pour l'autorisation d'envoi

Si vous voulez créer une stratégie pour l'autorisation d'envoi personnalisée et l'attacher à une identité, vous disposez des options suivantes :

- Utilisation de l'API Amazon SES – Créez une stratégie dans un éditeur de texte, puis attachez-la à l'identité à l'aide de l'API `PutIdentityPolicy` décrite dans le document Référence d'API Amazon Simple Email Service.
- Utilisation de la console Amazon SES – Créez une stratégie dans un éditeur de texte et attachez-la à une identité en la collant dans l'éditeur de stratégie personnalisée de la console Amazon SES. La procédure suivante décrit cette méthode.

Pour créer une stratégie pour l'autorisation d'envoi personnalisée en utilisant l'éditeur de stratégie personnalisé.

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES sur la page https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).

3. Dans le conteneur Identities (Identités) sur l'écran Verified identities (Identités vérifiées), sélectionnez l'identité vérifiée pour laquelle vous souhaitez autoriser l'expéditeur délégué à envoyer en votre nom.
4. Dans l'écran des détails de l'identité vérifiée que vous avez sélectionnée à l'étape précédente, choisissez l'onglet Authorization (Autorisation).
5. Dans le panneau Authorization policies (Stratégies d'autorisation), choisissez Create policy (Créer une stratégie), puis sélectionnez Create custom policy (Créer une stratégie personnalisée) depuis le menu déroulant.
6. Dans le volet Policy document (Document de la stratégie), saisissez ou collez le texte de votre stratégie au format JSON. Vous pouvez également utiliser le générateur de stratégies pour créer rapidement la structure de base d'une stratégie, puis la personnaliser ici.
7. Choisissez Apply Policy (Appliquer la stratégie). (Si vous avez besoin de modifier votre politique personnalisée, il suffit de cocher sa case à cocher sous l'onglet Authorization (Autorisation), choisir Edit (Modifier), et effectuer vos modifications dans le panneau Document de politique pour finir par Save changes (Enregistrer les modifications)).
8. (Facultatif) Si votre expéditeur délégué souhaite également utiliser une rubrique SNS dont il est propriétaire, pour recevoir des notifications de commentaires lorsqu'il reçoit des retours à l'expéditeur ou des réclamations, ou lorsque les e-mails sont délivrés, vous devrez configurer sa rubrique SNS dans cette identité vérifiée. (Votre expéditeur délégué devra partager avec vous son ARN de rubrique SNS.) Sélectionnez l'onglet Notifications et sélectionnezEdit (Modifier) dans le conteneur Feedback notifications (Notifications de commentaire) :

    a. Dans le panneau Configure SNS topics (Configuration des rubriques SNS(, l'un des champs de retour, (retour à l'expéditeur, réclamation ou remise), sélectionnez SNS topic you don't own (Sujet SNS que vous ne possédez pas) et saisissez le SNS topic ARN (ARN de rubrique SNS) détenu et partagé avec vous par votre expéditeur délégué. (Seul l'expéditeur délégué recevra ces notifications, car il est propriétaire de la rubrique SNS ; vous, en tant que propriétaire de l'identité, ne les recevrez pas.)

    b. (Facultatif) Si vous souhaitez que votre notification de rubrique inclue les en-têtes de l'e-mail d'origine, cochez la case Include original email headers (Incluez les en-têtes d'e-mail d'origine) située directement sous le nom de rubrique SNS de chaque type de commentaires. Cette option est disponible uniquement si vous avez affecté une rubrique Amazon SNS au type de notification associé. Pour en savoir plus sur le contenu des en-têtes de l'e-mail d'origine, consultez l'objet `mail` dans Contenu des notifications .

c. Sélectionnez Save Changes (Enregistrer les modifications). L'application des modifications que vous apportez à vos paramètres de notification peut prendre quelques minutes.

d. (Facultatif) Étant donné que votre expéditeur délégué recevra des notifications de rubriques Amazon SNS pour les retours à l'expéditeur et les réclamations, vous pouvez désactiver entièrement les notifications par e-mail si vous ne souhaitez pas recevoir de commentaires concernant les envois de cette identité. Pour désactiver les commentaires par e-mail pour les retours à l'expéditeur et les réclamations, sous l'onglet Notifications, dans le conteneur Email Feedback Forwarding (Transfert de commentaires par e-mail), choisissez Edit (Modifier), décochez la case Enabled (Activé), et choisissez Save changes (Enregistrer les modifications). Les notifications de statut de livraison seront désormais envoyées uniquement aux rubriques SNS appartenant à votre expéditeur délégué.

Exemples de stratégies d'envoi

Une autorisation d'envoi vous permet de spécifier les conditions précises selon lesquelles vous autorisez des expéditeurs délégués à effectuer un envoi en votre nom.

Les conditions et exemples suivants vous montrent comment écrire des stratégies pour contrôler différents aspects de l'envoi :

- Conditions spécifiques à l'envoi de l'autorisation
- Spécification de l'expéditeur délégué
- Restriction de l'adresse d'expédition
- Restriction de l'heure à laquelle le délégué peut envoyer un e-mail
- Limitation de l'action d'envoi d'e-mails
- Restriction du nom d'affichage de l'expéditeur de l'e-mail
- Utilisation de plusieurs instructions

Conditions spécifiques à l'envoi de l'autorisation

Une condition est une restriction qui s'applique à l'autorisation contenue dans l'instruction. La partie de l'instruction qui spécifie les conditions peut être la plus détaillée. Une clé est une caractéristique spécifique qui constitue la base pour une restriction d'accès (par exemple, la date et l'heure de la demande).

Vous utilisez à la fois les conditions et les clés afin d'exprimer la restriction. Par exemple, si vous voulez empêcher l'expéditeur délégué d'effectuer des demandes à Amazon SES en votre nom

après le 30 juillet 2019, vous devez utiliser la condition appelée `DateLessThan`. Vous utilisez la clé appelée `aws:CurrentTime` et la définissez sur la valeur `2019-07-30T00:00:00Z`.

Vous pouvez utiliser l'une des clés AWS générales répertoriées dans la section Available Keys (Clés disponibles) du Guide de l'utilisateur IAM, ou l'une des clés suivantes, spécifiques à SES, qui sont utiles pour les stratégies d'autorisation d'envoi :

Clé de condition	Description
`ses:Recipients`	Restreint les adresses des destinataires, qui incluent les adresses « To: », « CC » et « BCC ».
`ses:FromAddress`	Limite l'adresse d'expédition.
`ses:FromDisplayName`	Limite le contenu de la chaîne utilisée comme nom d'affichage de l'expéditeur (parfois appelé « nom d'expéditeur convivial »). Par exemple, le nom d'afficha ge « John Doe <johndoe@example.com> » est John Doe.
`ses:FeedbackAddress`	Limite l'adresse de retour, qui est l'adresse à laquelle les retours à l'expéditeur et les réclamations peuvent vous être envoyés via le transfert de commentaires par e-mail. Pour en savoir plus sur le transfert de commentaires par e-mail, consultez Réception des notifications Amazon SES par e-mail.

Vous pouvez utiliser les conditions `StringEquals` et `StringLike` avec des clés Amazon SES. Ces conditions sont destinées à la recherche de chaîne sensible à la casse. Pour `StringLike`, les valeurs peuvent inclure un caractère générique (*) correspondant à plusieurs caractères ou un caractère générique (?) correspondant à un seul caractère n'importe où dans la chaîne. Par exemple, la condition suivante indique que l'expéditeur délégué peut uniquement effectuer des envois à partir d'une adresse d'expédition qui commence par invoicing et se termine par example.com :

```
"Condition": {
    "StringLike": {
      "ses:FromAddress": "invoicing*@example.com"
    }
```

```
}
```

Vous pouvez également utiliser la condition `StringNotLike` pour empêcher les expéditeurs délégués d'envoyer des e-mails à partir de certaines adresses e-mail. Par exemple, vous pouvez interdire l'envoi depuis admin@example.com, ainsi que des adresses similaires telles que « admin »@example.com, admin+1@example.com ou sender@admin.example.com, en incluant la condition suivante dans votre déclaration de stratégie :

```
"Condition": {
    "StringNotLike": {
      "ses:FromAddress": "*admin*example.com"
    }
 }
```

Pour de plus amples informations sur la spécification de conditions dans une stratégie, consultez Éléments de stratégie JSON IAM : Condition dans le Guide de l'utilisateur IAM.

Spécification de l'expéditeur délégué

Le mandataire, qui est l'entité à laquelle vous accordez l'autorisation, peut être un compte Compte AWS, un utilisateur AWS Identity and Access Management (IAM) ou un service AWS.

L'exemple suivant montre une stratégie simple qui permet à l'ID AWS 123456789012 d'envoyer des e-mails à partir de l'identité vérifiée example.com (avec Compte AWS 888888888888 comme propriétaire). L'instruction `Condition` de cette stratégie autorise uniquement le délégué (c'est-à-dire, l'ID AWS 123456789012) à envoyer des e-mails à partir de l'adresse marketing+.*@example.com, où * correspond à une chaîne que l'expéditeur souhaite ajouter après marketing+.

```
{
  "Id":"SampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeMarketer",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
```

```
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition":{
        "StringLike":{
          "ses:FromAddress":"marketing+.*@example.com"
        }
      }
    }
  ]
}
```

L'exemple de stratégie suivant accorde à deux utilisateurs IAM une autorisation d'envoi à partir de l'identité example.com. Les utilisateurs IAM sont spécifiés par leur Amazon Resource Name (ARN).

```
{
  "Id":"ExampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeIAMUser",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "AWS":[
          "arn:aws:iam::111122223333:user/John",
          "arn:aws:iam::444455556666:user/Jane"
        ]
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ]
    }
  ]
}
```

L'exemple de stratégie suivant accorde à Amazon Cognito l'autorisation d'envoi à partir de l'identité example.com.

```
{
  "Id":"ExampleAuthorizationPolicy",
```

```
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeService",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "Service":[
          "cognito-idp.amazonaws.com"
        ]
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "888888888888",
          "aws:SourceArn": "arn:aws:cognito-idp:us-east-1:888888888888:userpool/your-
user-pool-id-goes-here"
        }
      }
    }
  ]
}
```

L'exemple de stratégie suivant accorde l'autorisation à tous les comptes au sein d'une Organization AWS d'envoyer à partir de l'identité example.com. L'Organization AWS est spécifiée à l'aide de la clé de condition globale PrincipalOrgID.

```
{
  "Id":"ExampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeOrg",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":"*",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
```

```
      "Condition":{
        "StringEquals":{
          "aws:PrincipalOrgID":"o-xxxxxxxxxxx"
        }
      }
    }
  ]
}
```

Restriction de l'adresse d'expédition

Si vous utilisez un domaine vérifié, vous pouvez créer une stratégie permettant uniquement à l'expéditeur délégué d'envoyer à partir d'une adresse e-mail spécifiée. Pour restreindre l'adresse d'expédition, vous devez définir une condition au niveau de la clé appelée ses:FromAddress. La stratégie suivante permet à l'ID Compte AWS 123456789012 d'effectuer un envoi à partir de l'identité example.com, mais uniquement à partir de l'adresse e-mail sender@example.com.

```
{
  "Id":"ExamplePolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeFromAddress",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition":{
        "StringEquals":{
          "ses:FromAddress":"sender@example.com"
        }
      }
    }
  ]
}
```

Restriction de l'heure à laquelle le délégué peut envoyer un e-mail

Vous pouvez également configurer votre stratégie d'autorisation de manière à ce qu'un expéditeur délégué ne puisse envoyer des e-mails qu'à une certaine heure du jour ou qu'au sein d'une certaine période. Par exemple, si vous prévoyez d'envoyer votre campagne par e-mail pendant le mois de septembre 2021, vous pouvez utiliser la stratégie suivante pour restreindre la capacité du délégué à n'envoyer les e-mails qu'au cours de ce seul mois.

```
{
  "Id":"ExamplePolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"ControlTimePeriod",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition":{
        "DateGreaterThan":{
          "aws:CurrentTime":"2021-08-31T12:00Z"
        },
        "DateLessThan":{
          "aws:CurrentTime":"2021-10-01T12:00Z"
        }
      }
    }
  ]
}
```

Limitation de l'action d'envoi d'e-mails

Avec Amazon SES, les expéditeurs peuvent envoyer un e-mail au moyen de deux actions : `SendEmail` et `SendRawEmail`. Tout dépend du degré de contrôle que l'expéditeur souhaite avoir sur le format de l'e-mail. Les stratégies d'autorisation d'envoi vous permettent de limiter l'expéditeur

délégué à l'une de ces deux actions. Toutefois, de nombreux propriétaires d'identité laissent à l'expéditeur délégué la possibilité de définir les détails des appels d'envoi d'e-mail en autorisant les deux actions dans leurs stratégies.

> **Note**
>
> Si vous souhaitez autoriser l'expéditeur délégué à accéder à Amazon SES via l'interface SMTP, vous devez choisir `SendRawEmail` au minimum.

Si votre cas d'utilisation vous impose de limiter l'action, incluez uniquement l'une des actions dans votre stratégie d'autorisation d'envoi. L'exemple suivant montre comment limiter l'action à `SendRawEmail`.

```
{
  "Id":"ExamplePolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"ControlAction",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
      "Action":[
        "ses:SendRawEmail"
      ]
    }
  ]
}
```

Restriction du nom d'affichage de l'expéditeur de l'e-mail

Certains clients de messagerie affichent le nom « convivial » de l'expéditeur de l'e-mail (si l'en-tête de l'e-mail l'indique) à la place de l'adresse d'expédition effective. Par exemple, le nom d'affichage « John Doe <johndoe@example.com> » est John Doe. Vous pouvez par exemple envoyer des e-mails à partir de user@example.com, mais préférer que les destinataires voient que l'e-mail provient de Marketing et non de user@example.com. La stratégie suivante permet à l'ID Compte AWS

123456789012 d'effectuer des envois à partir de l'identité example.com, mais uniquement si le nom complet de l'adresse d'expédition contient Marketing.

```
{
  "Id":"ExamplePolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeFromAddress",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition":{
        "StringLike":{
          "ses:FromDisplayName":"Marketing"
        }
      }
    }
  ]
}
```

Utilisation de plusieurs instructions

Votre stratégie d'autorisation d'envoi peut inclure plusieurs instructions. L'exemple de stratégie suivant comporte deux instructions. La première instruction autorise deux Comptes AWS à effectuer des envois à partir de sender@example.com aussi longtemps que l'adresse d'expédition et l'adresse de commentaire utilisent toutes deux le domaine example.com. La deuxième instruction autorise un utilisateur IAM à envoyer des e-mails à partir de sender@example.com, à condition que l'adresse e-mail du destinataire appartienne au domaine example.com.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
```

```
      "Sid":"AuthorizeAWS",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:999999999999:identity/sender@example.com",
      "Principal":{
        "AWS":[
          "111111111111",
          "222222222222"
        ]
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition":{
        "StringLike":{
          "ses:FromAddress":"*@example.com",
          "ses:FeedbackAddress":"*@example.com"
        }
      }
    },
    {
      "Sid":"AuthorizeInternal",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:999999999999:identity/sender@example.com",
      "Principal":{
        "AWS":"arn:aws:iam::333333333333:user/Jane"
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition":{
        "ForAllValues:StringLike":{
          "ses:Recipients":"*@example.com"
        }
      }
    }
  ]
}
```

Communication des informations d'identité à l'expéditeur délégué pour l'autorisation d'envoi Amazon SES

Une fois que vous avez créé votre stratégie d'autorisation d'envoi et que vous l'avez attachée à votre identité, vous pouvez fournir l'ARN (Amazon Resource Name) de l'identité à l'expéditeur délégué. L'expéditeur délégué transmet cet ARN à Amazon SES dans l'opération d'envoi d'e-mail ou dans l'en-tête de l'e-mail. Pour trouver l'ARN de votre identité, procédez comme suit.

Pour trouver l'ARN d'une identité

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).
3. Dans la liste des identités, choisissez l'identité à laquelle vous avez attaché la stratégie d'autorisation d'envoi.
4. Dans le panneau Summary (Récapitulatif), la deuxième colonne, Amazon Resource Name (ARN), contiendra l'ARN de l'identité. Il se présente comme suit : arn:aws:ses:us-east-1:123456789012:identity/user@example.com. Copiez l'ARN dans son intégralité et communiquez-le à votre expéditeur délégué.

Tâches d'expéditeur délégué pour l'autorisation d'envoi Amazon SES

En tant qu'expéditeur délégué, vous envoyez des e-mails au nom d'une identité dont vous n'êtes pas propriétaire, mais que vous êtes autorisé à utiliser. Même si vous effectuez un envoi au nom du propriétaire de l'identité, les retours à l'expéditeur et les réclamations sont comptabilisés dans les métriques de retour à l'expéditeur et de réclamation de votre compte AWS, et le nombre de messages que vous envoyez est comptabilisé dans votre quota d'envoi. Il vous incombe également de demander l'augmentation du quota d'envoi dont vous pourriez avoir besoin pour envoyer les e-mails du propriétaire de l'identité.

En tant qu'expéditeur délégué, vous devez exécuter les opérations suivantes :

- Communication d'informations au propriétaire d'identité
- Utilisation de notifications d'expéditeur délégué
- Envoi d'e-mails au nom du propriétaire d'identité

Communication d'informations au propriétaire d'identité pour l'autorisation d'envoi Amazon SES

En tant qu'expéditeur délégué, vous devez fournir au propriétaire de l'identité soit votre ID de compte AWS, soit l'Amazon Resource Name (ARN) de votre utilisateur IAM, puisque vous enverrez des e-mails au nom du propriétaire de l'identité. Le propriétaire de l'identité a besoin des informations de votre compte afin de pouvoir créer une politique qui vous accorde l'autorisation d'envoyer à partir d'une de ses identités vérifiées.

Si vous souhaitez utiliser vos propres rubriques SNS, vous pouvez demander à votre propriétaire d'identité de configurer les notifications de commentaires pour les retours à l'expéditeur, les réclamations ou les remises à envoyer à une ou plusieurs de vos rubriques SNS. Pour ce faire, vous devrez partager votre ARN de rubrique SNS avec votre propriétaire d'identité de manière à ce qu'il puisse configurer votre rubrique SNS dans l'identité vérifiée à partir de laquelle il vous autorise à envoyer.

Les procédures suivantes expliquent comment trouver les informations de votre compte et les ARN de rubrique SNS à partager avec le propriétaire de votre identité.

Pour trouver votre ID de compte AWS

1. Connectez-vous à AWS Management Console via https://console.aws.amazon.com.
2. Dans le coin supérieur droit de la console, choisissez votre nom ou votre numéro de compte, puis choisissez My Account (Mon compte) dans la liste déroulante.
3. La page des paramètres du compte s'ouvre et affiche toutes les informations relatives à votre compte, y compris votre ID de compte AWS.

Pour trouver l'ARN de votre utilisateur IAM

1. Connectez-vous à la AWS Management Console et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, sélectionnez Users.
3. Dans la liste des utilisateurs, choisissez le nom d'utilisateur. La section Summary (Récapitulatif) affiche l'ARN de l'utilisateur IAM. L'ARN ressemble à l'exemple suivant : arn:aws:iam::123456789012:user/John.

Pour trouver l'ARN de votre rubrique SNS

1. Ouvrez la console Amazon SNS à partir de l'adresse https://console.aws.amazon.com/sns/v3/home.
2. Dans le panneau de navigation, sélectionnez Topics (Rubriques).
3. Dans la liste des sujets, les ARN des rubriques SNS sont affichés dans la colonne ARN. L'ARN ressemble à l'exemple suivant : arn:aws:sns:us-east-1:444455556666:my-sns-topic.

Utilisation de notifications d'expéditeur délégué pour l'autorisation d'envoi Amazon SES

En tant qu'expéditeur délégué des e-mails entre comptes, vous envoyez des e-mails au nom d'une identité dont vous n'êtes pas propriétaire, mais que vous êtes autorisé à utiliser. Toutefois, les retours à l'expéditeur et les réclamations sont toujours pris en compte dans vos métriques de retour à l'expéditeur et de réclamation, et non celles du propriétaire de l'identité.

Si le taux de retours à l'expéditeur ou de réclamations pour votre compte devient trop élevé, votre compte risque d'être placé sous contrôle ou de ne plus pouvoir envoyer d'e-mails. Pour cette raison, il est important que vous configuriez les notifications et mettiez en place un processus pour les surveiller. Vous devez également mettre en place un processus pour supprimer de vos listes de diffusion les adresses qui ont fait l'objet de retours à l'expéditeur ou de réclamations.

Par conséquent, en tant qu'expéditeur délégué, vous pouvez configurer Amazon SES pour qu'il envoie des notifications lorsque des événements de retour à l'expéditeur et de réclamation se produisent pour les e-mails que vous envoyez au nom des identités que vous ne possédez pas, mais que vous avez été autorisé à utiliser par le propriétaire. Vous pouvez également configurer la publication d'événements pour publier des notifications de rebond et de plainte sur Amazon SNS ou Firehose.

> **Note**
>
> Si vous configurez Amazon SES de façon à envoyer des notifications à l'aide d'Amazon SNS, vous êtes facturé selon les tarifs Amazon SNS standard pour les notifications que vous recevez. Pour en savoir plus, consultez la page Tarification d'Amazon SNS.

Créer une nouvelle notification d'expéditeur délégué

Vous pouvez mettre en place des notifications d'envoi de délégués soit avec des ensembles de configuration utilisant la publication d'événements, soit avec des identités vérifiées configurées avec vos propres rubriques SNS.

Les procédures sont données ci-dessous pour configurer un nouvel envoi délégué de notifications en utilisant l'une ou l'autre méthode :

- Publication d'événements au moyen d'un jeu de configurations
- Notifications de commentaires sur les rubriques SNS que vous possédez

Pour configurer la publication d'événements via un jeu de configurations pour l'envoi délégué

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Suivez la procédure fournie dans Créer des destination d'évenement.
3. Une fois que vous avez configuré la publication d'événements dans votre jeu de configurations, spécifiez le nom du jeu de configurations lorsque vous envoyez un e-mail en tant qu'expéditeur délégué à l'aide de l'identité vérifiée à partir de laquelle le propriétaire de l'identité vous a autorisé à envoyer. veuillez consulter Envoi d'e-mails au nom du propriétaire d'identité.

Pour configurer des notifications de commentaires sur les rubriques SNS que vous possédez pour l'envoi délégué

1. Une fois que vous avez décidé quelles rubriques SNS vous souhaitez utiliser pour les notifications de commentaires, suivez les procédures pour trouver l'ARN de votre rubrique SNS, copiez l'ARN complet et partagez-le avec le propriétaire de votre identité.
2. Demandez à votre propriétaire d'identité de configurer vos rubriques SNS pour les notifications de commentaires sur l'identité partagée à partir de laquelle il vous a autorisé à envoyer. (Le propriétaire de votre identité devra suivre les procédures données pour la configuration des rubriques SNS dans les procédures de politique d'autorisation.)

Envoi d'e-mails au nom du propriétaire d'identité pour l'autorisation d'envoi Amazon SES

En tant qu'expéditeur délégué, vous envoyez les e-mails de la même façon que les autres expéditeurs Amazon SES, sauf que vous fournissez l'Amazon Resource Name (ARN) de l'identité

que son propriétaire vous a autorisé à utiliser. Lorsque vous appelez Amazon SES pour envoyer l'e-mail, Amazon SES vérifie si l'identité que vous avez spécifiée est associée à une stratégie qui vous autorise à effectuer un envoi pour ladite identité.

Il existe différentes façon de spécifier l'ARN de l'identité au moment d'envoyer un e-mail. La méthode que vous utilisez varie selon que vous envoyez l'e-mail à l'aide des opérations de l'API Amazon SES ou de l'interface SMTP Amazon SES.

> **Important**
>
> Pour envoyer un e-mail avec succès, vous devez vous connecter au point de terminaison Amazon SES dans la région AWS dans laquelle le propriétaire d'identité a vérifié l'identité. De plus, les comptes AWS du propriétaire d'identité et de l'expéditeur délégué doivent être supprimés de l'environnement de test (sandbox) pour que l'un ou l'autre des comptes puisse envoyer des e-mails à des adresses non vérifiées. Pour plus d'informations, consultez Demande d'accès à la production (sortie du sandbox d'Amazon SES).

Utilisation de l'API Amazon SES

Comme n'importe quel expéditeur d'e-mails Amazon SES si vous accédez à Amazon SES par l'intermédiaire de l'API Amazon SES (que ce soit directement via HTTPS ou indirectement via le kit SDK AWS), vous avez le choix entre trois actions d'envoi d'e-mail : `SendEmail`, `SendTemplatedEmail` ou `SendRawEmail`. Le document Référence d'API Amazon Simple Email Service décrit en détail ces API, mais nous offrons ici une présentation des paramètres d'autorisation d'envoi.

SendRawEmail

Si vous souhaitez utiliser `SendRawEmail` afin de contrôler le format de vos e-mails, vous pouvez spécifier l'identité entre comptes de deux manières différentes :

- Transmettez les paramètres facultatifs à l'**`SendRawEmail`**API. Les paramètres requis sont décrits dans le tableau suivant :

Paramètre	Description
`SourceArn`	ARN de l'identité associée à la stratégie d'autorisation d'envoi qui vous permet d'effectuer un envoi pour

Paramètre	Description
	l'adresse e-mail spécifiée dans le paramètre `Source` de `SendRawEmail` . **Note** Si vous spécifiez uniquement `SourceArn` , Amazon SES définit les adresses d'expédition (From) et de chemin de retour (Return-Path (Chemin de retour)) avec l'identité spécifiée dans `SourceArn` .
`FromArn`	ARN de l'identité associée à la stratégie d'autorisation d'envoi qui vous permet de spécifier une adresse d'expédition déterminée dans l'en-tête de l'e-mail brut.
`ReturnPathArn`	ARN de l'identité associée à la stratégie d'autorisation d'envoi qui vous permet d'utiliser l'adresse e-mail spécifiée dans le paramètre `ReturnPath` de `SendRawEmail` .

- Incluez les en-têtes X-header dans l'e-mail. Les en-têtes X-header sont des en-têtes personnalisés que vous pouvez utiliser en plus des en-têtes d'e-mail standard (tels que les en-têtes From, Reply-To ou Subject). Amazon SES reconnaît trois en-têtes X-header que vous pouvez utiliser pour spécifier les paramètres d'autorisation d'envoi :

Important

N'incluez pas ces en-têtes X dans la signature DKIM, car Amazon SES les supprime avant l'envoi de l'e-mail.

En-tête X	Description
`X-SES-SOURCE-ARN`	Correspond à `SourceArn` .

En-tête X	Description
X-SES-FROM-ARN	Correspond à FromArn.
X-SES-RETURN-PATH-ARN	Correspond à ReturnPathArn .

Amazon SES supprime tous les en-têtes X-header de l'e-mail avant de l'envoyer. Si vous incluez plusieurs instances d'un en-tête X-header, Amazon SES utilise uniquement la première instance.

L'exemple suivant présente un e-mail qui comprend des en-têtes X d'autorisation d'envoi :

```
X-SES-SOURCE-ARN: arn:aws:ses:us-east-1:123456789012:identity/example.com
X-SES-FROM-ARN: arn:aws:ses:us-east-1:123456789012:identity/example.com
X-SES-RETURN-PATH-ARN: arn:aws:ses:us-east-1:123456789012:identity/example.com

From: sender@example.com
To: recipient@example.com
Return-Path: feedback@example.com
Subject: subject
Content-Type: multipart/alternative;
 boundary="----=_boundary"

------=_boundary
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit

body
------=_boundary
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 7bit

body
------=_boundary--
```

SendEmail et SendTemplatedEmail

Si vous utilisez l'opération SendEmail ou SendTemplatedEmail, vous pouvez spécifier l'identité entre comptes en transmettant les paramètres facultatifs ci-dessous. Vous ne pouvez pas utiliser la méthode d'en-tête X-header si vous utilisez l'opération SendEmail ou SendTemplatedEmail.

Paramètre	Description
`SourceArn`	ARN de l'identité associée à la stratégie d'autorisation d'envoi qui vous permet d'effectuer un envoi pour l'adresse e-mail spécifiée dans le paramètre `Source` de `SendEmail` ou `SendTemplatedEmail` .
`ReturnPathArn`	ARN de l'identité associée à la stratégie d'autorisation d'envoi qui vous permet d'utiliser l'adresse e-mail spécifiée dans le paramètre `ReturnPath` de `SendEmail` ou `SendTemplatedEmail` .

L'exemple suivant montre comment envoyer un e-mail qui inclut les attributs `SourceArn` et `ReturnPathArn` à l'aide de l'opération `SendEmail` ou `SendTemplatedEmail` et du kit SDK pour Python.

```
import boto3
from botocore.exceptions import ClientError

# Create a new SES resource and specify a region.
client = boto3.client('ses',region_name="us-east-1")

# Try to send the email.
try:
    #Provide the contents of the email.
    response = client.send_email(
        Destination={
            'ToAddresses': [
                'recipient@example.com',
            ],
        },
        Message={
            'Body': {
                'Html': {
                    'Charset': 'UTF-8',
                    'Data': 'This email was sent with Amazon SES.',
                },
            },
            'Subject': {
                'Charset': 'UTF-8',
```

```
                'Data': 'Amazon SES Test',
            },
        },
        SourceArn='arn:aws:ses:us-east-1:123456789012:identity/example.com',
        ReturnPathArn='arn:aws:ses:us-east-1:123456789012:identity/example.com',
        Source='sender@example.com',
        ReturnPath='feedback@example.com'
    )
# Display an error if something goes wrong.
except ClientError as e:
    print(e.response['Error']['Message'])
else:
    print("Email sent! Message ID:"),
    print(response['ResponseMetadata']['RequestId'])
```

Utilisation de l'interface SMTP Amazon SES

Lorsque vous utilisez l'interface SMTP Amazon SES pour l'envoi entre comptes, vous devez inclure les en-têtes `X-SES-SOURCE-ARN`, `X-SES-FROM-ARN` et `X-SES-RETURN-PATH-ARN` dans votre message. Transmettez ces en-têtes une fois que vous avez émis la commande `DATA` dans la conversation SMTP.

Envoi d'e-mails test dans Amazon SES avec le simulateur

Nous vous recommandons d'utiliser la console Amazon SES pour envoyer un e-mail de test avec Amazon SES. La console nécessitant que vous saisissez manuellement les informations, vous l'utiliserez uniquement pour envoyer des e-mails de test. Une fois que vous serez familiarisé avec Amazon SES, vous enverrez très probablement vos e-mails à l'aide de l'interface SMTP ou de l'API. Cependant, la console est utile pour surveiller votre activité d'envoi.

Les rubriques suivantes expliquent comment utiliser le simulateur de boîte aux lettres à partir de la console et manuellement en envoyant des e-mails :

- Utilisation du simulateur de boîte aux lettres à partir de la console
- Utilisation manuelle du simulateur de boîte aux lettres

Utilisation du simulateur de boîte aux lettres à partir de la console

> **Important**
>
> - Dans ce didacticiel, vous vous envoyez un e-mail depuis la console afin de vérifier si vous l'avez reçu. Pour d'autres essais ou pour des tests de charge, consultez Utilisation manuelle du simulateur de boîte aux lettres.
> - Les e-mails envoyés au simulateur de boîte aux lettres ne sont pas pris en compte dans votre quota d'envoi ou vos taux de retours à l'expéditeur et de réclamations. Ils n'affectent pas non plus les métriques Virtual Deliverability Manager.

Avant de suivre ces étapes, exécutez les tâches décrites dans Configuration d'Amazon Simple Email Service.

Pour envoyer un message e-mail test à partir de la console Amazon SES

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES sur la page https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Verified identities (Identités vérifiées).
3. Dans la table Identities (Identités), sélectionnez une identité e-mail vérifiée (en cliquant directement sur le nom de l'identité plutôt que sur sa case à cocher). Si vous n'avez pas d'identité e-mail vérifiée, consultez Création d'une identité d'adresse e-mail.
4. Sur la page de détails de l'identité e-mail sélectionnée, sélectionnez Send test email (Envoyer un e-mail test).
5. Pour Message details (Détails du message), choisissez l'option Email Format (Format d'e-mail). Les deux options sont les suivantes :

   - Formatted (Formaté) – Il s'agit de l'option la plus simple. Sélectionnez cette option si vous souhaitez simplement taper le texte de votre message dans la zone de texte Body (Corps). Lorsque vous envoyez l'e-mail, Amazon SES met le texte au format d'e-mail pour vous.
   - Raw (Brut) – Choisissez cette option si vous voulez envoyer un message plus complexe, par exemple un message qui inclut du texte au format HTML ou une pièce jointe. En raison de cette flexibilité, vous devez formater vous-même le message, comme décrit dans Envoi d'e-

mails bruts à l'aide de l'API Amazon SES v2, puis coller l'intégralité du message formaté, y compris les en-têtes, dans la zone de texte Body (Corps). Vous pouvez utiliser l'exemple suivant, qui contient du texte au format HTML, pour envoyer un e-mail de test à l'aide du format d'e-mail Raw (Brut). Copiez et collez ce message dans son intégralité dans la zone de texte Body (Corps). Assurez-vous qu'il n'y a pas de ligne vide entre l'en-tête `MIME-Version` et l'en-tête `Content-Type` ; une ligne vide entre ces deux lignes entraîne un formatage de l'e-mail en tant que texte brut et non en tant que HTML.

```
Subject: Amazon SES Raw Email Test
MIME-Version: 1.0
Content-Type: text/html

<!DOCTYPE html>
<html>
<body>
<h1>This text should be large, because it is formatted as a header in HTML.</h1>
<p>Here is a formatted link: <a href="https://docs.aws.amazon.com/ses/latest/
DeveloperGuide/Welcome.html">Amazon Simple Email Service Developer Guide</a>.</p>
</body>
</html>
```

6. Choisissez le type de scénario d'e-mail simulé à tester dans la zone de liste Scenario.

   - Si vous choisissez Custom (Personnalisé) et si vous êtes toujours dans l'environnement de test (sandbox) Amazon SES, assurez-vous que l'adresse qui figure dans le champ Custom recipient (Destinataire personnalisé) est une adresse e-mail vérifiée. Pour de plus amples informations, veuillez consulter Création d'une identité d'adresse e-mail.

7. Remplissez les champs restants à votre convenance.
8. Choisissez Send Test Email (Envoyer l'e-mail de test).
9. Connectez-vous au client de messagerie de l'adresse à laquelle vous avez envoyé l'e-mail. Vous trouverez le message que vous avez envoyé.

Utilisation manuelle du simulateur de boîte aux lettres

Amazon SES comprend un simulateur de boîte aux lettres qui vous permet de tester le comportement de votre application dans différents scénarios d'envoi d'e-mails. Le simulateur de boîte aux lettres est utile quand, par exemple, vous devez tester une application d'envoi d'e-mails sans créer d'adresses

électroniques fictives ou lorsque vous avez besoin de déterminer le débit maximal de votre système sans affecter votre quota d'envoi quotidien.

Considérations Importantes

Considérez les fonctionnalités et limitations suivantes lorsque vous utilisez le simulateur de boîte aux lettres Amazon SES :

- Vous pouvez utiliser le simulateur de boîte aux lettres même si vous êtes dans l'environnement de test (sandbox) Amazon SES.
- Les e-mails envoyés au simulateur de boîte aux lettres (mailbox) sont limités par le taux maximal d'envois de votre compte, mais ils n'affectent pas vos quotas d'envoi quotidien. Par exemple, si votre compte est autorisé à envoyer jusqu'à 10 000 messages par période de 24 heures, et que vous envoyez 100 messages au simulateur de boîte aux lettres (mailbox), vous pouvez toujours envoyer jusqu'à 10 000 messages à des destinataires standard sans atteindre vos quotas d'envoi.
- Les e-mails envoyés au simulateur de boîte aux lettres (mailbox) n'affectent pas vos métriques de délivrabilité d'e-mails ou de réputation. Par exemple, si vous envoyez un grand nombre de messages à l'adresse de retour à l'expéditeur du simulateur de boîte aux lettres (mailbox), il n'affiche pas de message pour vous avertir que votre taux de retour à l'expéditeur est trop élevé sur la page de la console des métriques de réputation.
- À des fins de facturation, les e-mails envoyés au simulateur de boîte aux lettres Amazon SES sont les mêmes que tout autre e-mail que vous envoyez avec Amazon SES. En d'autres termes, nous facturerons la même quantité pour les messages que vous envoyez au simulateur de boîte aux lettres que pour ceux que vous envoyez à des destinataires standard.
- Le simulateur de boîte aux lettres (mailbox) prend en charge l'étiquetage, ce qui vous permet d'envoyer des e-mails à une même adresse du simulateur de boîte aux lettres (mailbox) de diverses manières, ou de voir comment votre application gère le Chemin de retour de l'enveloppe variable (VERP) Par exemple, vous pouvez envoyer un e-mail à bounce+label1@simulator.amazonses.com et à bounce+label2@simulator.amazonses.com pour voir si votre application parvient à faire correspondre un message de retour à l'expéditeur avec l'adresse ayant entraîné le retour.
- Si vous utilisez le simulateur de boîte aux lettres pour simuler plusieurs retours en provenance de la même demande d'envoi, Amazon SES combine les réponses de retour à l'expéditeur en une seule réponse.

Utilisation du simulateur de boîte aux lettres

Pour utiliser le simulateur de messagerie, recherchez le scénario dans le tableau suivant, puis envoyez un e-mail à l'adresse e-mail correspondante.

> **Note**
>
> Lorsque vous envoyez un e-mail à une adresse du simulateur de boîte aux lettres, vous devez l'envoyer via Amazon SES, à l'aide de l'AWS CLI, d'un kit SDK AWS, de la console Amazon SES, de l'interface SMTP Amazon SES ou de l'API Amazon SES. Le simulateur de boîte aux lettres email (mailbox) ne répond pas aux e-mails qu'il reçoit de sources externes.

Scénario simulé	Adresse e-mail
Livraison réussie : le fournisseur de messagerie du destinataire accepte votre e-mail. Si vous avez configuré les notifications de remise comme décrit dans Configuration de notifications d'événement pour Amazon SES, Amazon SES vous envoie une notification de livraison via Amazon Simple Notification Service (Amazon SNS).	success@simulator.amazonses.com
Retour à l'expéditeur : le fournisseur de messagerie du destinataire rejette votre e-mail avec un code de réponse SMTP 550 5.1.1 (« Unknown User »). Amazon SES génère une notification de retour à l'expéditeur et, selon la façon dont vous avez configuré votre compte, vous l'envoie par e-mail ou par l'intermédiaire d'une notification à une rubrique Amazon SNS. L'adresse e-mail de simulateur de boîte aux lettres (mailbox) n'est pas placée sur la liste de suppression Amazon SES, comme elle devrait normalement l'être en cas de message d'erreur définitif. La réponse de retour à l'expéditeur que	bounce@simulator.amazonses.com

Scénario simulé	Adresse e-mail
vous recevez de la part du simulateur de boîte aux lettres (mailbox) est conforme à RFC 3464. Pour plus d'informations sur la réception d'un commentaire de retour à l'expéditeur, consultez Configuration de notifications d'événement pour Amazon SES.	
Réponses automatiques : le fournisseur de messagerie du destinataire accepte votre e-mail et le transmet à la boîte de réception du destinataire. Le fournisseur de messagerie envoie une réponse automatique, comme un message « Absent du bureau » (Out of the office), à l'adresse indiquée dans l'en-tête Return-Path de l'e-mail ou à celle de l'envelop pe expéditeur (« MAIL FROM ») si l'en-tête Return-Path n'est pas présent. La réponse automatique que vous recevez de la part du simulateur de boîte aux lettres email (mailbox) est conforme à RFC 3834.	ooto@simulator.amazonses.com

Scénario simulé	Adresse e-mail
Réclamation : le fournisseur de messageri e du destinataire accepte votre e-mail et le transmet à la boîte de réception du destinata ire. Le destinataire décide que votre message est non sollicité et clique sur « Marquer comme indésirable » dans son client de messageri e. Amazon SES vous transmet ensuite la notification de réclamation par e-mail ou par l'intermédiaire d'une notification à une rubrique Amazon SNS, en fonction de la manière dont vous avez configuré votre compte. La réponse de réclamation que vous recevez de la part du simulateur de boîte aux lettres email (mailbox) est conforme à RFC 5965. Pour plus d'informations sur la réception d'un commentai re de réclamation, consultez Configuration de notifications d'événement pour Amazon SES.	complaint@simulator.amazonses.com
Adresse du destinataire sur la liste de suppression : Amazon SES génère un message d'erreur définitif comme si l'adresse du destinataire figurait sur la liste de suppressi on globale.	suppressionlist@simulator.amazonses.com

Test des événements de rejet

Chaque message envoyé via Amazon SES est analysé pour rechercher les virus. Si vous envoyez un message contenant un virus, Amazon SES accepte le message, détecte le virus et rejette l'ensemble du message. Lorsqu'un message est rejeté, Amazon SES arrête de le traiter et ne tente pas de le remettre au serveur de messagerie du destinataire. Il génère ensuite un événement Reject.

Le simulateur de boîte aux lettres d'Amazon SES n'inclut pas d'adresse pour le test d'événements de rejet. Cependant, vous pouvez tester les événements de rejet à l'aide d'un fichier de test EICAR (European Institute for Computer Antivirus Research). Ce fichier est une méthode standard de test

des logiciels antivirus en toute sécurité. Pour créer un fichier de test EICAR, collez le texte suivant dans un fichier :

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Enregistrez le fichier sous le nom de `sample.txt`, attachez-le à un e-mail, puis envoyer l'e-mail à une adresse vérifiée. Si l'e-mail ne présente pas d'autre problème, Amazon SES accepte le message, mais le rejette ensuite comme s'il contenait réellement un virus.

> **Note**
>
> Les e-mails rejetés, ainsi que ceux que vous envoyez à l'aide de la procédure ci-dessus, sont pris en compte dans votre quota d'envoi quotidien. Chaque message que vous envoyez est facturé, y compris les messages rejetés.

Pour en savoir plus sur les fichiers de test EICAR, consultez la page sur le fichier de test EICAR sur Wikipédia.

Utilisation des jeux de configuration dans Amazon SES

Les jeux de configuration sont des groupes de règles que vous pouvez appliquer à vos identités vérifiées. Une identité vérifiée est un domaine, un sous-domaine ou une adresse e-mail que vous utilisez pour envoyer des e-mails via Amazon SES. Lorsque vous appliquez un jeu de configurations à un e-mail, toutes les règles de ce jeu de configurations s'appliquent à celui-ci.

Vous pouvez utiliser des jeux de configurations pour appliquer les types de règles suivants à votre envoi d'e-mails et peut contenir un, deux ou aucun de ces types :

- Destinations des événements : vous permettent de publier des statistiques d'envoi d'e-mails, notamment le nombre d'envois, de livraisons, d'ouvertures, de clics, de rebonds et de plaintes concernant d'autres AWS produits pour chaque e-mail que vous envoyez. Par exemple, vous pouvez envoyer les statistiques de vos e-mails vers une destination Amazon Data Firehose, puis les analyser à l'aide d'Amazon Managed Service pour Apache Flink. Vous pouvez également envoyer des informations de retour à l'expéditeur et de réclamation à Amazon SNS, et recevoir immédiatement des notifications lorsque ces événements se produisent.
- Gestion des groupes d'adresses IP – Si vous louez des adresses IP dédiées pour une utilisation avec Amazon SES, vous pouvez créer des groupes pour ces adresses, appelés groupes d'adresses IP dédiées, à utiliser pour l'envoi de types spécifiques d'e-mails. Par exemple, vous pouvez associer ces pools d'IP dédiés à des jeux de configurations et en utiliser un pour l'envoi de communications marketing, et un autre pour l'envoi des e-mails transactionnels. Votre réputation d'expéditeur pour les e-mails transactionnels est ainsi isolée de vos e-mails marketing.

L'association d'un jeu de configurations à une identité vérifiée peut se faire de la manière suivante :

- incluez une référence au jeu de configurations dans les en-têtes de l'e-mail. Pour en savoir plus sur la spécification de jeux de configuration dans vos e-mails, consultez Spécification d'un jeu de configurations lors de l'envoi d'un e-mail.
- Spécifiez un jeu de configurations existant à utiliser comme jeu de configurations par défaut de l'identité, soit au moment de la création de celle-ci, soit plus tard lors de la modification d'une identité vérifiée. veuillez consulter Comprendre les jeux de configurations par défaut.

Table des matières

- Gestion des jeux de configurations Amazon SES
- Spécification d'un jeu de configurations lors de l'envoi d'un e-mail
- Affichage et exportation des métriques de réputation

Création de jeux de configuration dans SES

Vous pouvez utiliser la console SES, l'action `CreateConfigurationSet` dans l'API Amazon SES v2 ou la commande `aws sesv2 create-configuration-set` dans l'interface de ligne de commande Amazon SES v2 pour créer un jeu de configurations. Cette section explique comment créer des jeux de configuration à l'aide de la console SES et de l'interface de ligne de commande Amazon SES v2.

Créer un jeu de configurations (console)

Procédez de la manière suivante pour créer un jeu de configurations à l'aide de la console SES :

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Configuration sets (Jeux de configurations).
3. Choisissez Create set (Créer un jeu).
4. Entrez les détails suivants dans la section General details (Informations générales) :

    - Configuration set name (Nom du jeu de configurations) – Le nom pour le jeu de configurations. Le nom peut contenir jusqu'à 64 caractères alphanumériques : les lettres, les chiffres, les tirets (-) et les traits de soulignement (_) uniquement.
    - Sending IP pool (Envoi d'adresses IP) – Lorsque vous envoyez des e-mails à l'aide de ce jeu de configuration, les messages sont envoyés à partir des adresses IP dédiées du groupe affecté. Sélectionnez un groupe IP dans la liste.

    > **Note**
    >
    > La valeur par défaut (ses-default-dedicated-pool) contient des adresses IP dédiées qui n'ont été affectées à aucun autre groupe. Pour en savoir plus sur les groupes d'adresses IP, consultez Attribuer des groupes d'adresses.

- Options de suivi : cochez la case Utilisation d'un domaine de redirection personnalisé pour utiliser un domaine de redirection personnalisé pour gérer le suivi des ouvertures et des clics pour ce jeu de configurations, au lieu d'utiliser l'un des domaines SES.
  - Custom redirect domain – (Domaine de redirection personnalisé) — Avec un domaine de redirection personnalisé, vous pouvez entrer un sous-domaine personnalisé dans la zone (facultatif) ou sélectionner un domaine vérifié dans la liste.

> **Note**
>
> Les domaines de redirection personnalisés peuvent être spécifiés comme suit :
>
> - Les domaines de redirection doivent être configurés avant de choisir cette option. Pour plus d'instructions sur la sélection d'un domaine personnalisé pour gérer le suivi d'ouvertures et de clics, consultez Configuration de domaines personnalisés pour gérer le suivi des ouvertures et des clics.
> - Si vous souhaitez ensuite choisir d'utiliser un domaine de redirection personnalisé, vous devez l'indiquer lors de la création de votre jeu de configuration, ou ultérieurement en modifiant vos options de suivi pour le jeu de configuration.

- Advanced delivery options (Options de livraison avancées) – Choisissez la flèche à gauche pour développer la section des options de livraison avancées.
  - Protocole TLS (Transport Layer Security) : pour demander à SES d'établir une connexion sécurisée avec le serveur de messagerie de réception et d'envoyer des e-mails à l'aide du protocole TLS, sélectionnez l'option Obligatoire.

> **Note**
>
> SES prend en charge TLS 1.2 et recommande TLS 1.3. Pour en savoir plus, veuillez consulter la section Sécurité de l'infrastructure dans SES.

5. Entrez les détails suivants dans la section Reputation options (Options de réputation) :

- Mesures de réputation : utilisées pour suivre les indicateurs de rebond et de plainte CloudWatch pour les e-mails envoyés à l'aide de cet ensemble de configuration. (Des frais supplémentaires s'appliquent, voir Prix par métrique pour CloudWatch.)
  - Enabled (Activé) — Cochez cette case pour activer les métriques de réputation pour le jeu de configurations.

6. La section Suppression list options (Options de liste de suppression) fournit un ensemble de décisions permettant de définir une suppression personnalisée en commençant par l'option permettant d'utiliser ce jeu de configurations pour supplanter la suppression au niveau de votre compte. La carte logique de suppression au niveau du jeu de configurations vous aidera à comprendre les effets des combinaisons de remplacement. Ces sélections à plusieurs niveaux de remplacement peuvent être combinées pour implémenter trois niveaux de suppression différents :

   a. Use account-level suppression (Utiliser la suppression au niveau du compte) : ne remplace pas la suppression au niveau de votre compte et n'implémente aucune suppression au niveau du jeu de configurations. En fait, tout e-mail envoyé à l'aide de ce jeu de configurations utilisera simplement la suppression au niveau de votre compte. Pour cela :

      - Dans Suppression list settings (Paramètres de la liste de suppression), décochez la case Override account level settings (Remplacer les paramètres au niveau du compte).

   b. Do not use any suppression (N'utiliser aucune suppression) : remplace la suppression au niveau de votre compte sans activer la suppression au niveau du jeu de configurations. Cela signifie que tout e-mail envoyé à l'aide de ce jeu de configurations n'utilisera aucune suppression au niveau de votre compte ; en d'autres termes, toute suppression est annulée. Pour cela :

      i. Dans Suppression list settings (Paramètres de la liste de suppression), cochez la case Override account level settings (Remplacer les paramètres au niveau du compte).

      ii. Dans Suppression list (Liste de suppression), décochez la case Enabled (Activé).

   c. Use configuration set-level suppression (Utiliser la suppression au niveau du jeu de configurations) : remplace la suppression au niveau de votre compte par des paramètres de liste de suppression personnalisés définis dans ce jeu de configurations. Cela signifie que tout e-mail envoyé à l'aide de ce jeu de configurations utilisera uniquement ses propres paramètres de suppression et ignorera tous les paramètres de suppression au niveau du compte. Pour cela :

      i. Dans Suppression list settings (Paramètres de la liste de suppression), cochez la case Override account level settings (Remplacer les paramètres au niveau du compte).

      ii. Dans Suppression list (Liste de suppression), cochez la case Enabled (Activé).

      iii. Dans Specify the reason(s)... (Spécifiez la ou les raisons...), sélectionnez l'un des motifs de suppression à utiliser pour ce jeu de configurations.

7. La section Virtual Deliverability Manager options (Options Virtual Deliverability Manager) vous permet de définir des paramètres personnalisés concernant l'utilisation du suivi de l'engagement et de la livraison partagée optimisée par ce jeu de configurations en remplaçant leur définition dans vos paramètres de compte Virtual Deliverability Manager :

   a. Pour désactiver à la fois le suivi de l'engagement et la livraison partagée optimisée pour ce jeu de configurations :

      i. Cochez la case Override account level settings (Remplacer les paramètres au niveau du compte).

      ii. Assurez-vous que la case Enabled (Activé) n'est pas cochée à la fois pour Engagement tracking (Suivi de l'engagement) et Optimized shared delivery (Livraison partagée optimisée), puis choisissez Save changes (Enregistrer les modifications).

   b. Pour activer ou désactiver le suivi de l'engagement et/ou la livraison partagée optimisée pour ce jeu de configurations, procédez comme suit :

      i. Cochez la case Override account level settings (Remplacer les paramètres au niveau du compte).

      ii. Cochez ou décochez Enabled (Activé) pour Engagement tracking (Suivi de l'engagement) et/ou Optimized shared delivery (Livraison partagée optimisée), puis choisissez Save changes (Enregistrer les modifications).

   c. Pour revenir à vos paramètres de compte Virtual Deliverability Manager pour le suivi de l'engagement et la livraison partagée optimisée pour ce jeu de configurations :

      - Décochez la case Override account level settings (Remplacer les paramètres au niveau du compte), puis choisissez Save changes (Enregistrer les modifications).

8. Vous pouvez ajouter une ou plusieurs balise (s) dans la section Tags (Balises). Répétez les étapes suivantes pour chaque balise que vous souhaitez ajouter à votre jeu de configurations.

   a. Sélectionnez Add new tag (Ajouter une nouvelle balise).

   b. Saisissez la clé de balise.

   c. Entrez la Valeur de balise (facultatif).

   Pour supprimer une balise que vous avez saisie, choisissez Remove (Supprimez) pour cette balise. Vous pouvez entrer jusqu'à 50 balises.

9. Choisissez Create set (Créer un jeu) pour créer votre jeu de configurations.

Maintenant que vous avez créé votre jeu de configurations, vous avez la possibilité de définir des destinations d'événements pour votre jeu de configurations, ce qui permet la publication d'événements déclenchée sur les types d'événements que vous spécifiez pour la destination de l'événement. Un jeu de configurations peut comporter plusieurs destinations d'événements avec plusieurs types d'événements définis. veuillez consulter Création de destinations d'événement Amazon SES.

Créer un jeu de configurations (AWS CLI)

Vous pouvez créer un jeu de configuration à l'aide d'un fichier JSON en entrée dans dans la commande `aws sesv2 create-configuration-set` dans AWS CLI.

1. Créer un fichier JSON d'entrée CLI

   Utilisez votre outil d'édition de fichier favori pour créer un fichier JSON avec les clés suivantes, ainsi que des valeurs valides pour votre environnement, ou utilisez la commande `aws sesv2 create-configuration-set` de l'API SES v2 avec l'option `--generate-cli-skeleton` sans valeur spécifiée pour imprimer un échantillon de la structure JSON sur la sortie standard.

   Cet exemple utilise un fichier nommé`create-configuration-set.json` :

```
{
    "ConfigurationSetName": "sample-configuration-set",
    "TrackingOptions": {
        "CustomRedirectDomain": "some.domain.com"
    },
    "DeliveryOptions": {
        "TlsPolicy": "REQUIRE",
        "SendingPoolName": "sending pool"
    },
    "ReputationOptions": {
        "ReputationMetricsEnabled": true,
        "LastFreshStart": timestamp
    },
    "SendingOptions": {
        "SendingEnabled": true
    },
    "Tags": [
        {
            "Key": "tag key",
            "Value": "tag value"
        }
```

```
    ],
    "SuppressionOptions": {
        "SuppressedReasons": ["BOUNCE","COMPLAINT"]
    }
}
```

> **Note**
>
> - Vous devez inclure l'option `file://` au début du chemin du fichier JSON.
> - Le chemin d'accès du fichier JSON doit suivre la convention appropriée pour le système d'exploitation de base sur lequel vous exécutez la commande. En effet, Windows utilise la barre oblique inverse (\) pour faire référence au chemin du répertoire, et Linux utilise la barre oblique directe (/).

2. Exécutez la commande suivante en utilisant le fichier que vous avez créé en entrée.

```
aws sesv2 create-configuration-set --cli-input-json file://create-configuration-set.json
```

> **Note**
>
> Pour consulter la AWS CLI référence de cette commande, consultez create-configuration-set.

Gestion des jeux de configurations Amazon SES

Après avoir créé un jeu de configurations, vous pouvez le gérer avec les options d'affichage, de modification et de suppression en utilisant la console SES, l'API Amazon SES v2 et la CLI Amazon SES v2. Les jeux de configurations peuvent également être affectés à une identité vérifiée en tant que jeu de configurations par défaut appliqué chaque fois qu'un e-mail est envoyé à partir de cette identité.

Rubriques de cette section :

- Afficher, modifier et supprimer le jeu de configurations (console)
- Faire une liste des jeux de configuration (AWS CLI)
- Obtenez les détails du jeu de configuration (AWS CLI)

- Suppression d'un jeu de configurations (AWS CLI)
- Arrêtez l'envoi d'e-mails à partir d'un jeu de configuration (AWS CLI)
- Comprendre les jeux de configurations par défaut
- Création de destinations d'événement Amazon SES
- Attribuer des groupes d'adresses IP dans Amazon SES
- Configuration de domaines personnalisés pour gérer le suivi des ouvertures et des clics

Afficher, modifier et supprimer le jeu de configurations (console)

Accédez à la page détaillée d'un jeu de configurations existant

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Configuration sets (Jeux de configurations).
3. Pour afficher les détails d'un jeu de configuration, choisissez son Name (Nom) dans la liste du jeu de configuration. Vous accédez alors à la page des détails.

La page de description des jeux de configurations comporte deux onglets pour les détails du jeu de configuration, avec des panneaux dans chaque onglet où vous pouvez afficher, modifier ou supprimer de la manière suivante :

- Onglet Overview (Présentation)
  - General details (Renseignements généraux) — Ce panneau affiche les détails généraux du jeu de configuration :
    - Sending status (État d'envoi) (s'il est activé)
    - Configuration set name (Nom du jeu de configuration)
    - Envoi d'adresses IP
    - protocole TLS (Transport Layer Security)
    - Custom redirect domain (Domaine de redirection personnalisé)
  - Reputation options (Options de réputation) — Ce panneau affiche les détails relatifs à votre réputation d'envoi :
    - Reputation metrics (Métriques de réputation) (indique si vous effectuez le suivi des métriques)

    - Last fresh start (Dernier nouveau départ) (la date et l'heure à laquelle les métriques de réputation pour le jeu de configurations ont été réinitialisées pour la dernière fois)
- Suppression list options (Options de liste de suppression) : ce volet indique si vous remplacez la liste de suppression au niveau du compte par le jeu de configurations et, si c'est le cas, les détails de ce remplacement :
    - Suppression list settings (Paramètres de la liste de suppression) (indique le remplacement des paramètres au niveau du compte ; dans le cas contraire, il s'agit du seul élément affiché dans le volet)
    - Suppression list (Liste de suppression) (indique comment vous remplacez vos paramètres de compte, que la liste de suppression soit activée ou non)
    - Suppression reasons (Motifs de suppression) (indique si les retours à l'expéditeur et/ou les réclamations sont à l'origine de l'ajout des adresses e-mail des destinataires à votre liste de suppression)
- Virtual Deliverability Manager options (Options de Virtual Deliverability Manager) : ce volet indique si vous remplacez vos paramètres de compte Virtual Deliverability Manager pour le suivi de l'engagement et la livraison partagée optimisée par le jeu de configurations et, si c'est le cas, les détails du remplacement :
    - Engagement tracking (Suivi de l'engagement) (indique si le suivi de l'engagement est activé ou non)
    - Optimized shared delivery (Livraison partagée optimisée) (indique si la livraison partagée optimisée est activée ou non)
- Tags (Balises) – Ce panneau affiche toutes les balises que vous avez attachées au jeu de configuration.
    - Key (Clé)
    - Value (Valeur)

Vous pouvez effectuer les actions suivantes à partir des panneaux :

- Cliquez sur le bouton Edit (Modifier) ou, dans le cas du panneau Tags (Balises), le bouton Manage tags (Gérer les balises) pour modifier les détails respectifs de chaque panneau.
- Pour en savoir plus sur les champs, consultez la section connexe dans le document étapes Créer un jeu de configurations (console).

> **Tip**
>
> N'oubliez pas de faire une sauvegarde des modifications lorsque vous avez terminé. Choisissez Cancel (Annuler) pour revenir à la page de description du jeu de configurations sans enregistrer.

- Onglet Event destinations (Destinations de l'évènement)
  - All destinations (Toutes les destinations) (***`Nombre de destinations d'événements`***) – Ce panneau répertorie toutes les destinations d'événements que vous avez entrées pour votre jeu de configuration. Pour chaque destination, vous pouvez voir :
    - Name (Nom)
    - Destination (Destination)
    - Event types (Types d'événements
    - Event publishing (Publication d'événement

  Vous pouvez effectuer les actions suivantes à partir de ce panneau :

  - Ajoutez une nouvelle destination d'événement en choisissant le bouton Add destination (Ajouter une destination). Pour en savoir plus sur l'ajout d'une destination d'événement, consultez Création d'une destination d'événement.
  - Modifiez une destination d'événement existante en en sélectionnant le nom pour ouvrir l'écran de modification.
  - Supprime une destination d'événement existante en cochant la case en regard de son nom, puis en choisissant le bouton Delete (Supprimer).

En haut de la page de description de chaque jeu de configuration, et visible à partir de l'onglet Overview (Présentation) ou Events destination (Destination des événements), vous trouverez les options suivantes :

- Delete (Supprimer) — Ce bouton permet de supprimer votre jeu de configuration.
- Disable sending (Désactiver l'envoi) — Ce bouton permet d'arrêter d'envoyer des e-mails à partir de votre jeu de configuration.

Faire une liste des jeux de configuration (AWS CLI)

Vous pouvez utiliser la list-configuration-sets commande dans le AWS CLI pour générer une liste de tous les ensembles de configuration associés à votre compte dans la région actuelle, comme suit :

```
aws sesv2 list-configuration-sets
```

Obtenez les détails du jeu de configuration (AWS CLI)

Vous pouvez utiliser la get-configuration-set commande dans le pour AWS CLI obtenir des informations détaillées sur un ensemble de configuration spécifique, comme suit :

```
aws sesv2 get-configuration-set --configuration-set-name name
```

Suppression d'un jeu de configurations (AWS CLI)

Vous pouvez utiliser la delete-configuration-set commande du AWS CLI pour supprimer un ensemble de configuration spécifique, comme suit :

```
aws sesv2 delete-configuration-set --configuration-set-name name
```

Arrêtez l'envoi d'e-mails à partir d'un jeu de configuration (AWS CLI)

Vous pouvez utiliser la put-configuration-set-sending-options commande AWS CLI pour arrêter d'envoyer des e-mails à partir d'un ensemble de configuration spécifique, comme suit :

```
aws sesv2 put-configuration-set-sending-options --configuration-set-name name --no-
sending-enabled
```

Pour recommencer à envoyer, exécutez la même commande avec l'option `--sending-enabled` à la place, comme suit :

```
aws sesv2 put-configuration-set-sending-options --configuration-set-name name --
sending-enabled
```

Comprendre les jeux de configurations par défaut

Le concept d'affectation d'un jeu de configurations par défaut à utiliser par une identité vérifiée est expliqué dans cette section, pour aider à comprendre les avantages et le cas d'utilisation.

Un jeu de configurations par défaut applique automatiquement ses règles à tous les messages que vous envoyez à partir de l'identité d'adresse e-mail associée à ce jeu de configuration. Vous pouvez appliquer des jeux de configurations par défaut à la fois à l'adresse e-mail et aux identités de domaine pendant la création de l'identité ou a posteriori en tant que fonction de modification d'une identité existante.

Considérations relatives aux jeux de configurations par défaut

- Les jeux de configurations doivent d'abord être créés avant d'être associés à une identité.
- Les jeux de configurations par défaut ne seront appliqués que si l'identité est vérifiée.
- Une identité d'adresse e-mail ne peut être associée qu'à un seul jeu de configurations à la fois. Toutefois, vous pouvez appliquer le même jeu de configurations à plusieurs identités.
- Une configuration par défaut définie au niveau de l'adresse e-mail remplace une configuration par défaut définie au niveau du domaine. Par exemple, un jeu de configurations par défaut associé à joe@exemple.com remplace le jeu de configurations pour le domaine exemple.com.
- Une configuration par défaut définie au niveau du domaine s'applique à toutes les adresses e-mail de ce domaine (sauf si vous vérifiez des adresses spécifiques pour le domaine).
- Si vous supprimez un jeu de configurations désigné comme jeu de configuration par défaut pour une identité, puis que vous tentez d'envoyer un e-mail via cette identité, votre appel à Amazon SES échoue et affiche le message d'erreur « bad request » (requête erronée).
- Il n'est pas possible d'affecter un jeu de configurations par défaut à une identité vérifiée utilisée par un expéditeur délégué.
- La façon de spécifier un jeu de configurations existant à utiliser comme jeu de configurations par défaut de l'identité est en fait une fonction des identités vérifiées. Les instructions sont donc données dans les flux de travail de l'identité en conséquence :
  - Spécifier un jeu de configurations par défaut lors de la création d'identité – Suivez les instructions données dans l'étape 6 facultative pour soit le jeu de configurations par défaut d'identité de domaine, soit le jeu de configurations par défaut de l'identité e-mail, du chapitre Vérification des identités dans Amazon SES.
  - Spécifier un jeu de configurations par défaut pour une identité existante – suivez les étapes de la section Modification d'une identité à l'aide de la console avec ces détails pour l'étape 5 :
    a. Choisissez l'onglet Configuration set (jeu de configurations).
    b. Choisissez Edit (Modifier) dans le conteneur Default configuration set (jeu de configurations par défaut).

c. Sélectionnez la zone de liste et choisissez un jeu de configurations existant à utiliser par défaut.

d. Poursuivez en effectuant les étapes de la section Modification d'une identité à l'aide de la console.

> **Note**
>
> Si les métriques de réputation sont activées dans le jeu de configuration que vous attribuez par défaut, des frais supplémentaires seront facturés pour tout courrier envoyé à l'aide du jeu de configuration par défaut, voir Prix par métrique pour CloudWatch.

Création de destinations d'événement Amazon SES

Les destinations d'événements vous permettent de publier les actions de suivi des e-mails sortants suivantes vers d'autres AWS services à des fins de surveillance :

- Envois
- Échec du rendu
- Rejets
- Messages délivrés
- Messages d'erreur définitifs
- Réclamations
- Délais de livraison
- Abonnements
- Messages ouverts
- Clics

Pour en savoir plus sur la configuration de la publication d'événements, consultez the section called “Surveillance de l'envoi d'e-mails à l'aide de la publication d'événements”.

Création d'une destination d'événement

Une fois que vous avez créé un jeu de configurations, vous avez la possibilité de créer des destinations d'événements pour votre jeu de configurations, ce qui permet la publication

d'événements déclenchée sur les types d'événements que vous spécifiez pour la destination de l'événement. Un jeu de configurations peut comporter plusieurs destinations d'événements avec plusieurs types d'événements définis.

Si vous n'avez pas encore créé de jeu de configurations, consultez the section called “Créer des jeux de configuration”.

Les étapes suivantes montrent comment créer ou ajouter une destination d'événement à un jeu de configurations.

Pour créer ou ajouter une destination d'événement à l'aide de la console SES, procédez comme suit :

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Configuration sets (Jeux de configurations).
3. Choisissez le nom d'un jeu de configurations dans la colonne Name (Nom) pour accéder à ses détails.
4. Sélectionnez l'onglet Event destinations (Destinations d'évènement).
5. Choisissez Add destination (Ajouter une destination).
6. Sélectionnez les types d'événements.

   Les événements d'envoi d'e-mails sont des métriques relatives à votre activité d'envoi que vous pouvez mesurer à l'aide d'Amazon SES. Dans cette étape, vous sélectionnez les types d'événements d'envoi d'e-mails que vous souhaitez qu'Amazon SES publie sur votre destination d'événement.

   Pour en savoir plus sur les types évènement, veuillez consulter Surveillance de votre activité d'envoi Amazon SES.

   a. Choisissez les types d'événements à publier

      - Sending and delivery (Envoi et livraison) — Permet de choisir les types d'événements à publier, cochez les cases respectives ou choisissezSelect all (Sélectionner tout) pour publier tous les types d'événements.

Types d'événements

- Sends (Envois) La demande d'envoi a réussi et Amazon SES tente de remettre le message au serveur de messagerie du destinataire.
- Rendering failures (Échecs de rendu) – L'e-mail n'a pas été envoyé en raison d'un problème de rendu du modèle. Ce type d'événement peut se produire lorsqu'il manque des données du modèle ou lorsqu'il n'y a pas concordance entre les paramètres du modèle et les données. Ce type d'événement ne se produit que lorsque vous envoyez un e-mail à l'aide des opérations d'API `SendTemplatedEmail` ou `SendBulkTemplatedEmail`.
- Rejects (Rejets) – Amazon SES a accepté l'e-mail, a déterminé qu'il contenait un virus et l'a rejeté. Amazon SES n'a pas tenté de remettre l'e-mail au serveur de messagerie du destinataire.
- Deliveries (Messages délivrés) – Amazon SES a livré l'e-mail au serveur de messagerie du destinataire.
- Bounces (Retours à l'expéditeur) – Le serveur de messagerie du destinataire a définitivement rejeté l'e-mail. Soft bounces (Retours à l'expéditeur provisoires) sont inclus uniquement quand Amazon SES ne parvient pas à remettre l'e-mail après plusieurs tentatives au cours d'une période donnée.
- Complaints (Réclamations) — L'e-mail a été correctement remis au serveur de messagerie du destinataire, mais le destinataire l'a marqué comme courrier indésirable.
- Delivery delays (Retards de livraison) – L'e-mail n'a pas pu être remis au serveur de messagerie du destinataire car un problème temporaire s'est produit. Des retards de livraison peuvent se produire, par exemple lorsque la boîte de réception du destinataire est pleine ou lorsque le serveur de messagerie de réception rencontre un problème transitoire. (Ce type d'événement n'est pas pris en charge par Amazon Pinpoint.)
- Subscriptions (Abonnements) — L'e-mail a été envoyé avec succès, mais le destinataire a mis à jour les préférences d'abonnement en cliquant sur `List-Unsubscribe` dans l'en-tête de l'e-mail ou le lien `Unsubscribe` dans le pied-de-page. (Ce type d'événement n'est pas pris en charge par Amazon Pinpoint.)

- Open and click tracking (Ouvrez et cliquez sur le suivi) — Pour mesurer l'engagement des abonnés, cochez l'une ou les deux cases à cocher pour suivre les Messages ouverts et les Clics.
  - Opens (Ouvertures) – Le destinataire a reçu le message et l'a ouvert dans son client de messagerie.

- Clicks (Clics) – Le destinataire a cliqué sur un ou plusieurs liens contenus dans l'e-mail.

> **Note**
>
> Le paramètre Open and click event publishing (Publication d'événements d'ouverture et de clics) défini ici, ou dans tout autre jeu de configuration, n'affecte pas les options de suivi de l'engagement pour le tableau de bord de Virtual Deliverability Manager ; celles-ci sont définies par l'option Virtual Deliverability Manager's account settings (Paramètres du compte de Virtual Deliverability Manager) ou via des remplacements du jeu de configuration. Par exemple, si vous avez désactivé le suivi de l'engagement par le biais de Virtual Deliverability Manager, cela ne désactivera pas la publication des événements d'ouverture et de clic que vous avez configurés ici dans les destinations d'événements SES.

- Configuration set redirect domain (Domaine de redirection du jeu de configurations) – Ce champ apparaîtra et sera prérempli avec le nom du domaine de redirection personnalisé si vous en avez affecté un lors de la création du jeu de configurations.

> **Note**
>
> Vous pouvez mettre à jour la valeur Custom redirect domain (Domaine de redirection personnalisé) dans le jeu de configuration pour le suivi des ouvertures et des clics sous ce domaine. Pour ce faire, consultez Tracking options (Options de suivi) à l'étape 4 de Créer des jeux de configuration. Pour en savoir plus sur la configuration des domaines de messages ouverts et de clic personnalisés, consultez Configuration de domaines personnalisés pour gérer le suivi des ouvertures et des clics.

b. Choisissez Next (Suivant) pour continuer.

7. Spécifiez la destination

Une destination d'événement est un AWS service sur lequel les événements d'envoi d'e-mails peuvent être publiés. Le choix de la destination appropriée dépend du niveau de détail que vous souhaitez capturer et de la façon dont vous souhaitez recevoir les données.

a. Options de destination

- Type de destination : lorsque vous sélectionnez le bouton radio à côté du AWS service sur lequel vous souhaitez publier vos événements, un panneau de détails apparaît avec des champs correspondant au service. En sélectionnant les liens ci-dessous, vous trouverez des instructions sur le panneau de détails du service :
  - Amazon CloudWatch (Des frais supplémentaires s'appliquent, voir Prix par métrique pour CloudWatch.)
  - Amazon Data Firehose
  - Amazon EventBridge
  - Amazon Pinpoint (Ne prend pas en charge les types d'événements Retards de livraison ou Abonnements.)
  - Amazon SNS

  Pour en savoir plus sur l'utilisation du modèle de publication d'événements pour contrôler votre opération d'e-mail, consultez Surveillance de l'envoi d'e-mails à l'aide de la publication d'événements Amazon SES.
- Name (Nom) — Saisissez le nom de la destination pour ce jeu de configurations. Le nom ne peut contenir que des lettres, des chiffres et des traits d'union.
- Event publishing (Publication d'événement) — Pour activer la publication d'événements pour cette destination, sélectionnez la case Enabled (Activé).

b. Choisissez Next (Suivant) pour continuer.

8. Vérification

   Lorsque vous êtes satisfait de vos entrées, choisissezAdd destination (Ajouter une destination) pour ajouter votre destination d'événement.

Vous pouvez également créer une destination d'événement à l'aide de la console Amazon SES, de l'API Amazon SES v2 ou de la CLI Amazon SES v2.

Pour créer une destination d'événement à l'aide de l'API SES :

- Pour créer une destination d'événement à l'aide de l'API SES, voir `CreateConfigurationSetEventDestination`.

Modification, activation/désactivation ou suppression d'une destination d'événement

Suivez ces étapes pour modifier, désactiver/activer ou supprimer une destination d'événement à l'aide de la console SES :

Pour modifier, désactiver/activer ou supprimer une destination d'événement à l'aide de la console SES :

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Configuration sets (Jeux de configurations).
3. Choisissez le nom d'un jeu de configurations dans la colonne Name (Nom) pour accéder à ses détails.
4. Sélectionnez l'onglet Event destinations (Destinations d'événement) du jeu de configurations.
5. Sélectionnez le nom de la destination de l'événement sous la colonne Name (Nom).
6.
   - Pour modifier – Choisissez le bouton Edit (Modifier) sur le panneau correspondant pour l'ensemble de champs que vous souhaitez modifier et auquel vous souhaitez apporter des modifications, puis choisissez Save changes (Enregistrer les modifications).
   - Pour désactiver ou activer – Choisissez le bouton nommé Disable (Désactiver) ou Enable (Activer) situé dans l'angle supérieur droit.
   - Pour supprimer – Choisissez le bouton Delete (Supprimer) situé dans l'angle supérieur droit.

Vous pouvez également modifier, désactiver/activer ou supprimer une destination d'événement à l'aide de la console Amazon SES, de l'API Amazon SES v2 ou de la CLI Amazon SES v2.

Pour modifier, désactiver/activer ou supprimer une destination d'événement à l'aide de l'API SES :

1. Pour désactiver/activer une destination d'événement à l'aide de l'API SES, voir `UpdateConfigurationSetEventDestination`.
2. Pour supprimer une destination d'événement à l'aide de l'API SES, voir `DeleteConfigurationSetEventDestination`.

Attribuer des groupes d'adresses IP dans Amazon SES

Vous pouvez utiliser des groupes d'adresses IP pour créer des groupes d'adresses IP dédiées afin d'envoyer des types spécifiques d'e-mail. Vous pouvez également utiliser un groupe d'adresses IP partagées par tous les clients Amazon SES.

Lors de l'affectation d'un groupe d'adresses IP à un jeu de configurations, vous pouvez choisir parmi les options suivantes :

- Un groupe d'adresses IP dédiées spécifique – Lorsque vous sélectionnez un groupe d'adresses IP dédiées existant, les e-mails qui utilisent le jeu de configurations sont envoyés uniquement via les adresses IP dédiées appartenant à ce groupe. Pour les procédures de création :
  - de nouveaux groupes d'adresses IP standard, consultez Création de groupes d'adresses IP dédiées standard pour des adresses IP dédiées (standard).
  - de nouveaux groupes d'adresses IP gérées, consultez Création d'un groupe d'adresses IP gérées pour activer des adresses IP dédiées (gérées).
- ses-default-dedicated-pool – Ce groupe contient toutes les adresses IP dédiées pour votre compte qui n'appartiennent pas déjà à un groupe d'adresses IP. Si vous envoyez un e-mail à l'aide d'un jeu de configurations qui n'est pas associé à un groupe, ou si vous envoyez un e-mail sans spécifier de jeu de configurations, l'e-mail est envoyé à partir de l'une des adresses de ce groupe par défaut. Ce groupe est automatiquement géré par SES et ne peut pas être modifié.
- ses-shared-pool – Ce groupe contient un important jeu d'adresses IP qui sont partagées entre tous les clients Amazon SES. Cette option peut être utile lorsque vous avez besoin d'envoyer un e-mail qui n'est pas en adéquation avec vos comportements d'envoi habituels.

Attribution d'un groupe d'adresses IP à un jeu de configurations

Cette section fait référence aux procédures d'attribution et de modification des groupes IP dans un jeu de configuration à l'aide de la console Amazon SES.

- Pour affecter un groupe d'adresses IP à un jeu de configurations à l'aide de la console...
  - lors de la création d'un jeu de configurations — Voir Sending IP pool (Envoi du groupe d'adresses IP) à l'étape 4 de Créer des jeux de configuration
  - lors de la modification d'un jeu de configurations existant. – Sélectionnez le bouton Edit (Modifier) dans le panneau General details (Informations générales) du jeu de configurations sélectionné, et suivez les instructions pour Sending IP pool (Envoi du groupe d'adresses IP) à l'étape 4 de la section Créer des jeux de configuration

Configuration de domaines personnalisés pour gérer le suivi des ouvertures et des clics

Lorsque vous utilisez la publication d'événements pour capturer les événements d'ouvertures et de clics, Amazon SES apporte des modifications mineures sur les e-mails que vous envoyez. Pour capturer des événements ouverts, SES ajoute une image GIF transparente de 1 pixel par 1 pixel dans chaque e-mail envoyé via SES, qui inclut un nom de fichier unique pour chaque e-mail, et est hébergé sur un serveur exploité par SES. Lorsque l'image est téléchargée, SES peut indiquer exactement quel message a été ouvert et par qui.

Par défaut, ce pixel est inséré en bas de l'e-mail. Toutefois, les applications de certains fournisseurs de messagerie tronquent l'aperçu d'un e-mail lorsqu'il dépasse une certaine taille et peut fournir un lien pour afficher le reste du message. Dans ce scénario, l'image de suivi des pixels SES ne se charge pas et supprimera les taux d'ouverture que vous tentez de suivre. Pour contourner ce problème, vous pouvez éventuellement placer le pixel au début de l'e-mail, ou n'importe où ailleurs, en insérant l'espace réservé `{{ses:openTracker}}` dans le corps de l'e-mail. Une fois que SES aura reçu le message avec l'espace réservé, il sera remplacé par une image de pixel de suivi ouverte.

> **Important**
>
> Ajoutez un seul espace réservé `{{ses:openTracker}}`, car au-delà, un code d'erreur `400 BadRequestException` est renvoyé.

Pour capturer les événements de clics sur les liens, Amazon SES remplace les liens dans vos e-mails par des liens vers un serveur exploité par SES. Cela redirige immédiatement le destinataire vers sa destination initiale.

Vous avez également la possibilité d'utiliser vos propres domaines, plutôt que des domaines détenus et exploités par Amazon SES, pour créer une expérience plus cohérente pour vos destinataires, ce qui signifie que tous les indicateurs SES sont supprimés. Vous pouvez configurer plusieurs domaines personnalisés pour gérer les événements de suivi des ouvertures et des clics. Ces domaines personnalisés sont associés à des jeux de configuration. Lorsque vous envoyez un e-mail à l'aide d'un jeu de configuration, si ce jeu de configuration est configuré pour utiliser un domaine personnalisé, les liens d'ouvertures et de clics de cet e-mail utilisent automatiquement le domaine personnalisé spécifié dans ce jeu de configuration.

Cette section contient des procédures pour configurer un sous-domaine sur un serveur que vous possédez de façon à rediriger automatiquement les utilisateurs vers les serveurs de suivi des ouvertures et des clics gérés par Amazon SES. Trois étapes sont impliquées dans la configuration de ces domaines. Tout d'abord, vous configurez le sous-domaine lui-même, puis vous définissez un jeu de configurations pour utiliser le domaine personnalisé, puis vous définissez sa destination d'événement pour publier des événements ouverts et de clics. Cette rubrique contient les procédures de réalisation de ces étapes.

Toutefois, si vous souhaitez simplement activer le suivi des ouvertures ou des clics sans configurer de domaine personnalisé, vous pouvez définir directement les destinations des événements pour votre jeu de configuration, ce qui permet la publication d'événements déclenchée sur les types d'événements que vous spécifiez, y compris les événements d'ouverture et de clic. Un jeu de configurations peut comporter plusieurs destinations d'événements avec plusieurs types d'événements définis. veuillez consulter Création de destinations d'événement Amazon SES.

Partie 1 : Configurer un domaine pour gérer les redirections de liens d'ouvertures et de clics

Les procédures spécifiques de configuration d'un domaine de redirection varient en fonction de votre fournisseur d'hébergement web (et de votre réseau de diffusion de contenu, si vous utilisez un serveur HTTPS). Les procédures décrites dans les sections suivantes proposent des conseils généraux plutôt que des étapes spécifiques.

Option 1 : Configuration d'un domaine HTTP

Si vous avez l'intention d'utiliser un domaine HTTP pour gérer les liens d'ouvertures et de clics (plutôt qu'un domaine HTTPS), le processus de configuration du sous-domaine comprend seulement quelques étapes.

> **Note**
>
> Si vous configurez un domaine personnalisé qui utilise le protocole HTTP, et que vous envoyez un e-mail contenant des liens qui utilisent le protocole HTTPS, vos clients verront peut-être un message d'avertissement lorsqu'ils cliqueront sur les liens de votre e-mail. Si vous avez l'intention d'envoyer des e-mails contenant des liens qui utilisent le protocole HTTPS, vous devez utiliser un domaine HTTPS pour gérer les événements de suivi des clics.

Pour configurer un sous-domaine HTTP afin de gérer les liens d'ouvertures et de clics

1. Si vous ne l'avez pas déjà fait, créez un sous-domaine à utiliser pour les liens de suivi des ouvertures et des clics. Nous vous recommandons de créer un sous-domaine spécialement dédié à la gestion de ces liens.
2. Vérifiez le sous-domaine à utiliser avec Amazon SES. Pour plus d'informations, consultez Création d'une identité de domaine.
3. Modifiez le registre DNS du sous-domaine. Dans le registre DNS, ajoutez un nouvel registre CNAME qui redirige les requêtes vers le domaine de suivi Amazon SES. L'adresse vers laquelle vous redirigez dépend de la AWS région dans laquelle vous utilisez Amazon SES. Le tableau suivant contient une liste des domaines de suivi pour les régions AWS dans lesquelles Amazon SES est disponible.

AWS Région	AWS domaine de suivi
USA Est (Ohio)	`r.us-east-2.awstrack.me`
USA Est (Virginie du Nord)	`r.us-east-1.awstrack.me`
USA Ouest (Californie du Nord)	`r.us-west-1.awstrack.me`
USA Ouest (Oregon)	`r.us-west-2.awstrack.me`
Afrique (Le Cap)	`r.af-south-1.awstrack.me`
Asie-Pacifique (Jakarta)	`r.ap-southeast-3.awstrack.me`
Asie-Pacifique (Mumbai)	`r.ap-south-1.awstrack.me`
Asie-Pacifique (Osaka)	`r.ap-northeast-3.awstrack.me`
Asia Pacific (Seoul)	`r.ap-northeast-2.awstrack.me`
Asie-Pacifique (Singapour)	`r.ap-southeast-1.awstrack.me`
Asie-Pacifique (Sydney)	`r.ap-southeast-2.awstrack.me`
Asie-Pacifique (Jakarta)	r.ap-southeast-3.awstrack.me
Asie-Pacifique (Jakarta)	r.ap-southeast-3.awstrack.me

AWS Région	AWS domaine de suivi
Asie-Pacifique (Tokyo)	`r.ap-northeast-1.awstrack.me`
Canada (Centre)	`r.ca-central-1.awstrack.me`
Europe (Francfort)	`r.eu-central-1.awstrack.me`
Europe (Irlande)	`r.eu-west-1.awstrack.me`
Europe (Londres)	`r.eu-west-2.awstrack.me`
Europe (Milan)	`r.eu-south-1.awstrack.me`
Europe (Stockholm)	`r.eu-north-1.awstrack.me`
Israël (Tel Aviv)	`r.il-central-1.awstrack.me`
Moyen-Orient (Bahreïn)	`r.me-south-1.awstrack.me`
Amérique du Sud (Sao Paulo)	`r.sa-east-1.awstrack.me`
AWS GovCloud (US-Ouest)	`r.us-gov-west-1.awstrack.me`
AWS GovCloud (USA Est)	`r.us-gov-east-1.awstrack.me`

> **Note**
>
> En fonction de votre fournisseur d'hébergement web, l'application des modifications apportées à le registre DNS du sous-domaine peut prendre plusieurs minutes. Votre fournisseur d'hébergement web ou votre organisation TI peut fournir des informations supplémentaires sur ces retards.

Option 2 : Configuration d'un domaine HTTPS

Vous pouvez uniquement utiliser un domaine HTTPS pour suivre les clics sur les liens. Pour configurer un domaine HTTPS de manière à suivre les clics sur les liens, vous devez effectuer quelques étapes supplémentaires par rapport à celles requises pour configurer un domaine HTTP.

> **Note**
>
> Vous pouvez uniquement utiliser un domaine HTTPS pour suivre les clics sur les liens. Amazon SES prend uniquement en charge le suivi des ouvertures sur les domaines HTTP lors de l'utilisation d'un domaine personnalisé ; sinon, SES prend en charge le suivi des ouvertures sur HTTPS lorsqu'aucun domaine personnalisé n'est défini : les domaines détenus et exploités par SES seront donc utilisés de manière implicite.

Pour configurer un sous-domaine HTTPS afin de gérer les liens de clics

1. Créez un sous-domaine à utiliser pour les liens de suivi des clics. Nous vous recommandons de créer un sous-domaine spécialement dédié à la gestion de ces liens.
2. Vérifiez le sous-domaine à utiliser avec Amazon SES. Pour plus d'informations, consultez Création d'une identité de domaine.
3. Créez un nouveau compte auprès d'un réseau de diffusion de contenu (CDN), tel qu'Amazon CloudFront.
4. Configurez le CDN sur l'origine qui est le domaine de suivi SES, par exemple `r.us-east-1.awstrack.me`. Le CDN doit transmettre l'en-tête `Host` fourni par le demandeur à l'origine. Consultez cet article AWS re:Post pour en savoir plus. L'adresse que vous utilisez dépend de celle Région AWS que vous utilisez dans SES. Le tableau suivant contient une liste des domaines de suivi pour les AWS régions dans lesquelles SES est disponible.

AWS Région	AWS domaine de suivi
USA Est (Ohio)	`r.us-east-2.awstrack.me`
USA Est (Virginie du Nord)	`r.us-east-1.awstrack.me`
USA Ouest (Californie du Nord)	`r.us-west-1.awstrack.me`
USA Ouest (Oregon)	`r.us-west-2.awstrack.me`
Afrique (Le Cap)	`r.af-south-1.awstrack.me`
Asie-Pacifique (Jakarta)	`r.ap-southeast-3.awstrack.me`
Asie-Pacifique (Mumbai)	`r.ap-south-1.awstrack.me`

AWS Région	AWS domaine de suivi
Asie-Pacifique (Osaka)	`r.ap-northeast-3.awstrack.me`
Asia Pacific (Seoul)	`r.ap-northeast-2.awstrack.me`
Asie-Pacifique (Singapour)	`r.ap-southeast-1.awstrack.me`
Asie-Pacifique (Sydney)	`r.ap-southeast-2.awstrack.me`
Asie-Pacifique (Tokyo)	`r.ap-northeast-1.awstrack.me`
Canada (Centre)	`r.ca-central-1.awstrack.me`
Europe (Francfort)	`r.eu-central-1.awstrack.me`
Europe (Irlande)	`r.eu-west-1.awstrack.me`
Europe (Londres)	`r.eu-west-2.awstrack.me`
Europe (Milan)	`r.eu-south-1.awstrack.me`
Europe (Stockholm)	`r.eu-north-1.awstrack.me`
Israël (Tel Aviv)	`r.il-central-1.awstrack.me`
Moyen-Orient (Bahreïn)	`r.me-south-1.awstrack.me`
Amérique du Sud (Sao Paulo)	`r.sa-east-1.awstrack.me`
AWS GovCloud (US-Ouest)	`r.us-gov-west-1.awstrack.me`
AWS GovCloud (USA Est)	`r.us-gov-east-1.awstrack.me`

5. Si vous utilisez Route 53 pour gérer la configuration DNS de votre domaine et en CloudFront tant que CDN, créez un enregistrement Alias dans Route 53 qui fait référence à votre CloudFront distribution (par exemple d111111abcdef8.cloudfront.net). Pour en savoir plus, reportez-vous à la section Création de registres à l'aide de la console Amazon Route 53 dans le Guide du développeur Amazon Route 53.

   Sinon, dans la configuration DNS de votre sous-domaine, ajoutez un registre CNAME qui fait référence à l'adresse de votre CDN.

6. Obtenez un certificat SSL auprès d'une autorité de certification approuvée. Le certificat doit couvrir le sous-domaine que vous avez créé à l'étape 1, ainsi que le CDN que vous avez configuré lors des étapes 3 à 5. Chargez le certificat sur le CDN.

Partie 2 : Définition d'un jeu de configuration pour se référer à un domaine personnalisé de suivi des ouvertures et des clics

Une fois que vous avez configuré votre domaine afin de gérer les redirections de suivi des ouvertures et des clics, vous devez spécifier votre domaine personnalisé dans le jeu de configuration. Vous pouvez effectuer cela à l'aide de la console Amazon SES ou de l'opération d'API `CreateConfigurationSetTrackingOptions`.

Cette section présente les procédures à suivre pour effectuer ces tâches à l'aide de la console Amazon SES. Pour plus d'informations sur l'utilisation de l'API, consultez la section CreateConfigurationSetTrackingOptions du manuel Amazon Simple Email Service API Reference.

- Pour spécifier un domaine de redirection personnalisé à l'aide de la console...
  - lors de la création d'un jeu de configurations — voir Options de suivi à l'étape 4 deCréer des jeux de configuration
  - lors de la modification d'un jeu de configurations existant. – Sélectionnez le bouton Edit (Modifier) dans le panneau General details (Informations générales) du jeu de configurations sélectionné, et suivez les instructions pour Tracking options (Options de suivi) à l'étape 4 de la section Créer des jeux de configuration

Partie 3 : Sélection des types d'événements Ouvrir et Cliquer dans les destinations d'événements de votre jeu de configurations

Après avoir spécifié votre domaine personnalisé dans le jeu de configurations, vous devez sélectionner des types d'événements ouverts et/ou cliquer dans une destination d'événement ajoutée à votre jeu de configurations. Vous pouvez effectuer cela à l'aide de la console Amazon SES ou de l'opération d'API `CreateConfigurationSetEventDestination`.

- Pour sélectionner des types d'événements ouvrir/cliquer à l'aide de la console...
  - lors de la création d'une nouvelle destination d'événement – Voir Suivi des ouvertures et des clic à l'étape 6 de the section called “Création d'une destination d'événement”.

- lors de la modification d'une destination d'événement existante – Sélectionnez le bouton Edit (Modifier) situé dans le panneau Event types (Types d'événements) de la destination de l'événement sélectionnée à l'étape 6 de the section called “Modification, activation/désactivation ou suppression d'une destination d'événement”

Spécification d'un jeu de configurations lors de l'envoi d'un e-mail

Pour utiliser un jeu de configurations lors de l'envoi d'un e-mail, vous devez transmettre le nom du jeu de configurations dans les en-têtes de l'e-mail. Toutes les méthodes Amazon SES d'envoi d'e-mails (y compris l'AWS CLI, les kits SDK AWS et l'interface SMTP Amazon SES) vous permettent de transmettre un jeu de configurations dans les en-têtes de l'e-mail que vous envoyez.

Si vous utilisez l'interface SMTP ou l'opération d'API `SendRawEmail`, vous pouvez spécifier un jeu de configurations en incluant l'en-tête suivant dans votre e-mail (remplacez *`ConfigSet`* par le nom du jeu de configurations que vous souhaitez utiliser) :

```
X-SES-CONFIGURATION-SET: ConfigSet
```

Ce guide comprend des exemples de code pour envoyer des e-mails à l'aide des kits SDK AWS et de l'interface SMTP Amazon SES. Chacun de ces exemples inclut une méthode de spécification d'un jeu de configurations. Pour connaître step-by-step les procédures d'envoi d'e-mails contenant des références à des ensembles de configuration, consultez les rubriques suivantes :

- Envoi d'e-mails via Amazon SES à l'aide d'un AWS SDK
- Utilisation de l'interface SMTP d'Amazon SES pour envoyer des e-mails

Affichage et exportation des métriques de réputation

Amazon SES exporte automatiquement vers Amazon CloudWatch les informations relatives aux taux globaux de rebond et de réclamations pour l'ensemble de votre compte. Vous pouvez utiliser ces métriques pour créer des alarmes ou pour suspendre automatiquement l'envoi d'e-mails à l'aide d'une fonction Lambda. CloudWatch

Vous pouvez également exporter les métriques de réputation pour des ensembles de configuration individuels vers CloudWatch. L'exportation de données de réputation au niveau du jeu de configurations vous offre davantage de contrôle sur votre réputation d'expéditeur.

Cette section inclut les procédures d'exportation des données de réputation pour des ensembles de configuration individuels à CloudWatch l'aide de l'API Amazon SES.

Activation de l'exportation des mesures de réputation

Pour lancer l'exportation des métriques de réputation pour un jeu de configurations, utilisez l'opération d'API `UpdateConfigurationSetReputationMetricsEnabled`. Pour accéder à l'API Amazon SES, nous vous recommandons d'utiliser le AWS CLI ou l'un des AWS SDK.

Cette procédure suppose que le AWS CLI est installé sur votre ordinateur et correctement configuré. Pour plus d'informations sur l'installation et la configuration du AWS CLI, consultez le guide de AWS Command Line Interface l'utilisateur.

Pour activer l'exportation des métriques de réputation pour un jeu de configurations

- Sur la ligne de commande, entrez la commande suivante :

  ```
  aws ses update-configuration-set-reputation-metrics-enabled --configuration-set-
  name ConfigSet --enabled
  ```

  Remplacez *ConfigSet*la commande précédente par le nom du jeu de configuration pour lequel vous souhaitez commencer à exporter des métriques de réputation.

Désactivation de l'exportation des métrique de réputation

Vous pouvez également utiliser l'opération d'API `UpdateConfigurationSetReputationMetricsEnabled` pour désactiver l'exportation des métriques de réputation pour un jeu de configurations.

Pour désactiver l'exportation des métriques de réputation pour un jeu de configurations

- Sur la ligne de commande, entrez la commande suivante :

  ```
  aws ses update-configuration-set-reputation-metrics-enabled --configuration-set-
  name ConfigSet --no-enabled
  ```

  Remplacez *ConfigSet*la commande précédente par le nom du jeu de configuration pour lequel vous souhaitez désactiver l'exportation des métriques de réputation.

Adresses IP dédiées pour Amazon SES

Lorsque vous créez un nouveau compte Amazon SES, par défaut vos e-mails sont envoyés à partir d'adresses IP partagées avec d'autres utilisateurs SES. Vous pouvez également utiliser des adresses IP dédiées qui sont réservées à votre usage exclusif en les louant moyennant des frais supplémentaires. Cela vous donne un contrôle total sur votre réputation d'expéditeur et vous permet d'isoler votre réputation pour différents segments au sein des programmes de messagerie. Amazon SES propose deux méthodes pour mettre en service et gérer une adresse IP dédiée :

- Standard : fait référence aux adresses IP dédiées que vous configurez et gérez manuellement, y compris en les préparant et en les mettant à l'échelle manuellement, ainsi qu'en les introduisant ou en les sortant manuellement des groupes d'adresses IP. (Ces adresses étaient auparavant appelées adresses IP dédiées dans SES.)
- Gérée : fait référence aux adresses IP dédiées qui sont automatiquement configurées en votre nom par SES pour vous permettre de commencer à utiliser rapidement et facilement des adresses IP dédiées gérées par SES. Elles sont préparées automatiquement et individuellement pour chaque FSI, et s'adaptent automatiquement en fonction de votre volume d'envoi afin de garantir l'utilisation optimale de vos adresses IP dédiées, en fonction de la manière dont vous envoyez des e-mails.

Lorsque vous choisissez entre des adresses IP partagées et les deux types d'adresses IP dédiées définies ci-dessus, choisissez celles qui offrent le plus d'avantages par rapport au type, au volume et aux modèles de courrier électronique que vous envoyez. Pour vous aider dans votre décision, ces avantages sont résumés dans le tableau suivant. Choisissez un élément dans la colonne Avantage pour obtenir des informations supplémentaires.

Avantage	Adresses IP partagées	Adresses IP dédiées (standard)	Adresses IP dédiées (gérées)
Prêt à l'emploi immédiatement	Oui	Non	Non
Configuration supplémentaire requise	Non	Oui	Oui

Avantage	Adresses IP partagées	Adresses IP dédiées (standard)	Adresses IP dédiées (gérées)
Adresses IP et réputation isolées des autres clients de SES	Non	Oui	Oui
La capacité augmente automatiquement à mesure que le trafic augmente	Non	Non	Oui
Adapté aux clients effectuant des envois prévisibles et continus	Oui	Oui	Oui
Adapté aux clients effectuant des envois moins prévisibles	Oui	Non	Oui
Adapté aux clients effectuant des envois volumineux	Oui	Oui	Oui
Adapté aux clients effectuant des envois peu volumineux	Oui	Non	Non
Coûts mensuels supplémentaires	Non	Oui	Oui
Contrôle total de la réputation de l'expéditeur	Non	Oui	Oui
Isolation de la réputation par type d'e-mail, destinataire ou d'autres facteurs	Non	Oui	Oui

Avantage	Adresses IP partagées	Adresses IP dédiées (standard)	Adresses IP dédiées (gérées)
Adresses IP connues qui ne changent jamais	Non	Oui	Non

> **Important**
>
> Si vous ne prévoyez pas d'envoyer de gros volumes d'e-mails de façon régulière et prévisible, nous vous recommandons d'utiliser des adresses IP partagées. Si vous souhaitez utiliser des adresses IP dédiées dans les cas où vos envois sont très irréguliers, la meilleure option est d'utiliser des adresses IP dédiées (gérées).

Configuration simplifiée

Adresses IP partagées : vous n'avez pas besoin d'effectuer de configuration supplémentaire. Votre compte SES est prêt à envoyer des e-mails dès que vous avez vérifié une adresse e-mail et que vous avez quitté l'environnement de test (sandbox).

Adresses IP dédiées (standard) : vous devez envoyer une demande via le AWS Support Center et éventuellement configurer des pools d'adresses IP dédiés.

Adresses IP dédiées (gérées) : vous n'avez pas besoin de soumettre de demande d'adresses IP dédiées. Elles sont automatiquement allouées lorsque vous vous inscrivez et effectuez une procédure pas à pas unique pour créer votre groupe dédié géré.

Gestion de réputation

La réputation de l'adresses IP repose principalement sur les schémas et les volumes d'envoi historiques. Une adresse IP qui envoie des volumes de messages homogènes sur une longue période jouit généralement d'une bonne réputation.

Adresses IP partagées : partagées entre plusieurs clients SES, ces adresses envoient collectivement un volume important d'e-mails et AWS gère avec soin le trafic sortant afin de maximiser la réputation des adresses IP partagées.

Adresses IP dédiées (standard) : après le préchauffage, vos adresses IP sont isolées du pool partagé de SES et vous préservez votre propre réputation d'expéditeur en envoyant des volumes d'e-mails constants et prévisibles.

Adresses IP dédiées (gérées) : après le préchauffage de vos nouvelles adresses IP, elles sont isolées du pool partagé de SES et vous conservez votre propre réputation d'expéditeur. Il y a l'avantage supplémentaire de suivre la réputation de chaque FAI et de planifier de manière optimale les envois sortants en conséquence. Ainsi, tout en préservant votre réputation d'expéditeur, cette automatisation contribue à améliorer la délivrabilité globale et à réduire les taux de rebond par rapport à des charges de travail équivalentes sur des adresses IP dédiées configurées manuellement.

> **Note**
>
> Pour obtenir des informations sur les données SNDS (Smart Network Data Services) pour vos adresses IP dédiées, consultez Métriques SNDS pour les adresses IP dédiées.

Prévisibilité des envois

Une adresse IP présentant un historique d'envois d'e-mails cohérent a meilleure réputation qu'une adresse IP qui commence à envoyer soudainement d'importants volumes d'e-mails sans historique d'envois antérieurs.

Adresses IP partagées : idéales pour les modèles d'envoi d'e-mails qui ne suivent pas un schéma prévisible. Avec les adresses IP partagées, vous pouvez accroître ou alléger vos envois d'e-mails quand la situation l'exige.

Adresses IP dédiées (standard) : vous devez préparer les adresses en envoyant une quantité d'e-mails qui augmente progressivement chaque jour. Le processus de préparation de nouvelles adresses IP est décrit dans Préparation des adresses IP dédiées (standard). Une fois que vos adresses IP dédiées ont été préparées, vous devez ensuite maintenir une logique d'envoi cohérente.

Adresses IP dédiées (gérées) : vos adresses IP dédiées sont automatiquement réchauffées pour chaque adresse IP du pool géré à l'aide d'une stratégie de préchauffage adaptative (associée au pool partagé SES) qui prend en compte les modèles d'envoi réels afin d'optimiser le préchauffage pour chaque FAI individuellement. Le pool d'adresses IP géré évolue automatiquement par fournisseur de services Internet en fonction de l'utilisation et de la prise en compte des politiques spécifiques du fournisseur de services Internet.

Volume d'e-mails sortants

Adresses IP partagées : idéal pour les clients qui envoient de faibles volumes d'e-mails.

Adresses IP dédiées (standard) | Adresses IP dédiées (gérées) : toutes deux conviennent aux clients qui envoient de grands volumes d'e-mails. La plupart des fournisseurs de services Internet (FSI) suivent la réputation d'une adresse IP donnée seulement s'ils reçoivent un volume important de courrier en provenance de cette adresse. Pour chaque ISP auprès duquel vous souhaitez cultiver une réputation, vous devez envoyer plusieurs centaines d'e-mails sur une période de 24 heures au moins une fois par mois. Dans certains cas, les deux types d'adresses IP dédiées peuvent également fonctionner pour de plus petits volumes d'e-mails. Par exemple, elles peuvent être une solution si vous envoyez des e-mails à un petit groupe bien défini de destinataires, dont les serveurs de messagerie acceptent ou rejettent les messages en se basant sur une liste d'adresses IP spécifiques plutôt que sur la réputation des adresses IP.

Coûts supplémentaires

Adresses IP partagées : incluses dans la tarification SES standard.

Adresses IP dédiées (standard) : elles sont disponibles moyennant des frais mensuels supplémentaires pour chaque adresse IP que vous louez. Pour obtenir des informations sur la tarification, consultez la page de tarification SES.

Adresses IP dédiées (gérées) : elles sont disponibles moyennant un tarif mensuel standard (quel que soit le nombre d'adresses IP nécessaires) et moyennant des frais d'utilisation par message. Pour obtenir des informations sur la tarification, consultez la page de tarification SES.

Contrôle de la réputation de l'expéditeur

Adresses IP partagées : votre réputation d'expéditeur est contrôlée par SES.

Adresses IP dédiées (standard) | Adresses IP dédiées (gérées) : votre réputation d'expéditeur est entièrement sous votre contrôle. Votre compte SES est le seul en mesure d'envoyer des e-mails de ces adresses. C'est pourquoi votre réputation d'expéditeur est déterminée par vos pratiques d'envoi d'e-mails. En outre, les adresses IP dédiées (gérées) surveillent activement les adresses IP sortantes utilisées pour l'envoi d'e-mails en utilisant les adresses IP les plus performantes afin d'améliorer la délivrabilité des e-mails à vos destinataires. Les données d'utilisation peuvent être mises en évidence

à l'aide de services supplémentaires tels que CloudWatch les métriques Amazon et les tableaux de bord intégrés à Amazon SES.

Aptitude à isoler la réputation d'expéditeur

Adresses IP partagées : votre réputation d'expéditeur est définie au niveau du compte et ne peut pas être isolée.

Adresses IP dédiées (standard) | Adresses IP dédiées (gérées) : vous pouvez isoler votre réputation d'expéditeur pour différents composants dans votre programme de messagerie en créant des groupes d'adresses IP dédiées, que vous pouvez utiliser pour l'envoi de types spécifiques d'e-mails. Par exemple, vous pouvez créer un groupe d'adresses IP dédiées pour l'envoi d'e-mails marketing et un autre pour l'envoi d'e-mails transactionnels.

Adresses IP connues et fixes

Adresses IP partagées : vous ne savez pas quelles adresses IP sont utilisées par SES pour envoyer vos e-mails et elles peuvent changer à tout moment.

Adresses IP dédiées (standard) : vous pouvez trouver les valeurs des adresses qui envoient vos e-mails sur la page Dedicated IPs (Adresses IP dédiées) de la console SES. Cela est dû au fait que les adresses IP dédiées sont statiques.

Adresses IP dédiées (gérées) : SES configurera automatiquement le nombre optimal d'adresses IP dédiées en fonction de vos modèles d'envoi. Cela signifie que les adresses IP dédiées de votre groupe ne sont pas visibles et augmenteront ou diminueront de manière dynamique en fonction de la demande.

Adresses IP dédiées (standard) dans Amazon SES

Les adresses IP dédiées (standard) sont des adresses IP dédiées que vous configurez et gérez manuellement dans SES. Elles sont différentes de celles qui sont configurées et gérées automatiquement à l'aide de la fonctionnalité SES the section called “Gérées”. En plus de vous permettre de contrôler totalement votre réputation d'expéditeur à l'aide des adresses IP dédiées, les adresses IP dédiées (standard) vous permettent de gérer entièrement vos adresses IP dédiées, y compris en les préparant, en les faisant monter en puissance et en gérant le groupe d'adresses IP.

Les adresses IP dédiées (standard) et les adresses IP dédiées (gérées) font toutes deux référence à des adresses IP dédiées que vous louez dans SES moyennant des frais supplémentaires, mais

diffèrent quant à leur mise en œuvre et à leur gestion. Bien qu'elles présentent des avantages communs, elles offrent toutes deux des avantages uniques en fonction de votre type d'envoi de courrier, comme indiqué dans Adresses IP dédiées.

Les rubriques de cette section expliquent comment configurer et gérer manuellement des adresses IP dédiées (standard) dans SES.

Rubriques

- Demande et abandon d'adresses IP dédiées (standard)
- Préparation des adresses IP dédiées (standard)
- Création de groupes d'adresses IP dédiées standard pour des adresses IP dédiées (standard)

Demande et abandon d'adresses IP dédiées (standard)

Pour utiliser des adresses IP dédiées (standard), vous devez d'abord les demander. Lorsque vous n'en avez plus besoin, vous devez les abandonner. Demandez et abandonnez des adresses IP dédiées (standard) via le Centre AWS Support. Nous facturons sur votre compte des frais mensuels supplémentaires pour chaque adresse IP dédiée standard que vous louez pour une utilisation avec Amazon SES. Il n'y a aucun engagement minimum attenant à l'utilisation d'adresses IP dédiées (standard).

Pour plus d'informations sur les coûts associés aux adresses IP dédiées (standard), consultez Tarification Amazon SES.

Pour obtenir une liste de toutes les régions où Amazon SES est actuellement disponible, consultez Régions et points de terminaison Région AWS du Référence générale d'Amazon Web Services. Pour en savoir plus sur le nombre de zones de disponibilité présentes dans chaque Région AWS, consultez Infrastructure mondiale AWS.

Demande d'adresses IP dédiées (standard)

Vous pouvez demander autant d'adresses IP dédiées (standard) que vous en avez besoin en créant une demande d'augmentation de quotas de service dans le Centre de support AWS.

Pour demander des adresses IP dédiées (standard)

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES sur la page https://console.aws.amazon.com/ses/.

2. Dans le panneau de navigation de gauche, choisissez Dedicated IPs (Adresses IP dédiées).
3. Effectuez l'une des actions suivantes :

   a. S'il n'existe pas d'adresses IP dédiées dans votre compte :

      - La page d'intégration Dedicated IPs (Adresses IP dédiées) s'affiche. Dans le volet Dedicated IPs (standard) overview (Présentation des adresses IP dédiées (standard)), choisissez Request dedicated IPs (Demander des adresses IP dédiées).

        La page Create case (Créer un dossier) s'ouvre dans la console de support AWS.

   b. Si vous avez des adresses IP dédiées existantes sur votre compte :

      i. Sélectionnez l'onglet Standard IP pools (Groupes d'adresses IP standard) sur la page Dedicated IPs (Adresses IP dédiées).
      ii. Dans le panneau Standard overview (Présentation standard), choisissez Request or relinquish Standard dedicated IPs (Demander ou abandonner des adresses IP dédiées standard).

        La page Create case (Créer un dossier) s'ouvre dans la console de support AWS.
4. Sous Create case (Créer une demande), sélectionnez la carte Service limit increase (Augmentation de limite de service) en haut de la page.
5. Sous Case details (Détails du cas), complétez les sections suivantes :

   - Pour Type de limite (Type de limite), gardez SES Service Limits (Limites de service SES).
   - Pour Mail Type (Type d'e-mail), choisissez le type d'e-mail que vous prévoyez d'envoyer par l'intermédiaire de votre adresse IP dédiée. Si plusieurs valeurs s'appliquent, choisissez l'option qui s'applique à la majorité des e-mails que vous prévoyez d'envoyer.
   - Pour Website URL (URL du site web), saisissez l'URL de votre site web. Ces informations nous aident à mieux comprendre le type de contenu que vous prévoyez d'envoyer.
   - Pour Describe, in detail, how you will only send to recipients who have specifically requested your mail (Décrivez, en détail, la façon dont vous enverrez uniquement aux destinataires qui ont demandé votre courrier de manière spécifique), fournissez une réponse adaptée à votre cas d'utilisation.
   - Pour Describe, in detail, the process that you will follow when you receive bounce and complaint notifications (Décrivez en détail le processus que vous suivrez lorsque vous recevrez des notifications de retour à l'expéditeur et de réclamation), fournissez une réponse adaptée à votre cas d'utilisation.

- Pour Will you comply with AWS Service Terms and AUP (Respecterez-vous les conditions de service et la stratégie d'utilisation acceptable AWS), choisissez l'option qui s'applique à votre cas d'utilisation.

6. Sous Requests (Demandes), complétez les sections suivantes :

   - Pour Region (Région), choisissez la Région AWS à laquelle votre demande s'applique.
   - Pour Limit (Limite), conservez Desired Dedicated IP (Adresse IP dédiée souhaitée).
   - Pour New limit value (Nouvelle valeur de limite), saisissez le nombre d'adresses IP dédiées que vous devez implémenter pour votre cas d'utilisation.

   > **Note**
   >
   > Si vous souhaitez demander des adresses IP dédiées à utiliser dans une autre Région AWS, choisissez Add another request (Ajouter une autre demande), puis renseignez les champs Region (Région), Limit (Limite) et New limit value (Nouvelle valeur de limite) pour la Région AWS supplémentaire. Répétez cette procédure pour chaque Région AWS dans laquelle vous souhaitez utiliser des adresses IP dédiées.

7. Sous Case description (Description de la demande), pour Use case description (Description du cas d'utilisation), indiquez que vous souhaitez demander des adresses IP dédiées. Si vous souhaitez demander un nombre spécifique d'adresses IP dédiées, mentionnez-le également. Si vous ne spécifiez pas un nombre d'adresses IP dédiées, nous fournirons le nombre d'adresses IP dédiées qui sont nécessaires pour répondre aux exigences de taux d'envoi que vous avez spécifiées à l'étape précédente.

   Ensuite, décrivez comment vous prévoyez d'utiliser les adresses IP dédiées pour envoyer des e-mails avec Amazon SES. Incluez des informations sur les raisons pour lesquelles vous voulez utiliser des adresses IP dédiées, et non des adresses IP partagées. Ces informations nous aident à mieux comprendre votre cas d'utilisation.

8. Sous Options de contact, pour Langue de contact préférée, choisissez si vous souhaitez recevoir les communications pour cette demande en anglais ou en japonais.

9. Lorsque vous avez terminé, choisissez Submit (Soumettre).

Une fois le formulaire envoyé, nous évaluons votre demande. Si nous acceptons votre demande, nous y répondons dans le Centre de support pour confirmer que vos nouvelles adresses IP dédiées sont associées à votre compte.

Abandon d'adresses IP dédiées standard

Si vous utilisez des adresses IP dédiées que vous ne souhaitez plus voir associées à votre compte, la procédure suivante montre comment les abandonner en créant une demande dans le Centre de support AWS.

> **Important**
>
> Le processus d'abandon d'une adresse IP dédiée ne peut pas être annulé. Si vous abandonnez une adresse IP dédiée au milieu d'un mois, nous calculons le taux d'utilisation mensuel de cette adresse IP dédiée, en fonction du nombre de jours qui se sont écoulés dans le mois en cours.

Pour abandonner des adresses IP dédiées (standard)

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES sur la page https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation de gauche, choisissez Dedicated IPs (Adresses IP dédiées).
3. Sélectionnez l'onglet Standard IP pools (Groupes d'adresses IP standard) sur la page Dedicated IPs (Adresses IP dédiées).
4. Dans le panneau Standard overview (Présentation standard), choisissez Request or relinquish Standard dedicated IPs (Demander ou abandonner des adresses IP dédiées standard).
5. Sous Case details (Détails du cas), pour Limit type (Type de limite), conservez SES Service Limits (Limites de service SES).

   > **Note**
   >
   > Les cases restantes de cette section ne s'appliquent pas à l'abandon d'adresses IP dédiées. Laissez les vide.

6. Sous Requests (Demandes), complétez les sections suivantes :

- Pour Region (Région), choisissez la Région AWS à laquelle votre demande d'abandon s'applique.

  > **Note**
  >
  > Les adresses IP dédiées sont uniques pour chaque Région AWS. Il est donc important de choisir la Région AWS à laquelle l'adresse IP dédiée est associée.

- Pour Limit (Limite), conservez Desired Dedicated IP (Adresse IP dédiée souhaitée).
- Pour New limit value (Nouvelle valeur de limite), entrez la valeur de votre choix. Le nombre que vous saisissez ici n'est pas important : vous spécifiez le nombre d'adresses IP dédiées que vous souhaitez abandonner à l'étape suivante.

  > **Note**
  >
  > Une adresse IP dédiée unique ne peut être utilisée que dans une seule Région AWS. Si vous souhaitez abandonner des adresses IP dédiées que vous utilisez dans d'autres Régions AWS, choisissez Add another request (Ajouter une autre demande). Renseignez ensuite les champs Region (Région), Limit (Limite) et New limit value (Nouvelle valeur de limite) pour la Région AWS supplémentaire. Répétez cette procédure pour chaque adresse IP dédiée que vous souhaitez abandonner.

7. Sous Case description (Description de la demande), pour Use case description (Description du cas d'utilisation), indiquez que vous souhaitez abandonner des adresses IP dédiées existantes. Si vous louez actuellement plusieurs adresses IP dédiées, incluez le nombre d'adresses IP dédiées que vous souhaitez abandonner.
8. Sous Options de contact, pour Langue de contact préférée, choisissez si vous souhaitez recevoir les communications pour cette demande en anglais ou en japonais.
9. Lorsque vous avez terminé, choisissez Submit (Soumettre).

Après avoir reçu votre demande, nous vous envoyons un message qui vous demande de confirmer que vous souhaitez abandonner vos adresses IP dédiées. Une fois que vous avez confirmé que vous souhaitez abandonner des adresses IP, nous les supprimons de votre compte.

Préparation des adresses IP dédiées (standard)

Lorsqu'ils déterminent s'ils doivent accepter ou refuser un message, les fournisseurs de services de messagerie tiennent compte de la réputation de l'adresse IP qui l'a envoyé. L'un des facteurs qui contribue à la réputation d'une adresse IP est si celle-ci présente un historique d'envoi d'e-mails de grande qualité. Les fournisseurs de messagerie sont moins susceptibles d'accepter des messages de nouvelles adresses IP qui ont peu ou pas d'historique. Un e-mail envoyé à partir d'adresses IP avec peu ou pas de l'historique risque de se retrouver dans les dossiers de courrier indésirable des destinataires ou d'être complètement bloqué.

Lorsque vous commencez à envoyer des e-mails à partir d'une nouvelle adresse IP dédiée, vous devez augmenter progressivement la quantité d'e-mails que vous envoyez de cette adresse avant de l'utiliser à sa pleine capacité. Ce processus est nommé préparation de l'adresse IP.

La quantité de temps nécessaire pour préparer une adresse IP varie selon le fournisseur de messagerie. Pour certains fournisseurs de messagerie, vous pouvez établir une réputation positive en deux semaines environ, tandis que pour d'autres fournisseurs, cela peut prendre jusqu'à six semaines. Lors de la préparation d'une nouvelle adresse IP dédiée, vous devez envoyer des e-mails à vos utilisateurs les plus actifs afin de vous assurer que le taux de réclamations reste bas. Vous devez également examiner soigneusement les messages de retour à l'expéditeur et envoyer moins d'e-mails si vous recevez un nombre élevé de blocage ou de notifications de limitation. Pour en savoir plus sur la surveillance des retours à l'expéditeur, consultez Surveillance de votre activité d'envoi Amazon SES.

Préparation automatique des adresses IP dédiées (standard)

Lorsque vous demandez des adresses IP dédiées (standard), Amazon SES les prépare automatiquement pour améliorer la remise des e-mails que vous envoyez. La fonctionnalité de préparation automatique des adresses IP est activée par défaut. SES prépare automatiquement vos adresses IP dédiées en augmentant progressivement le nombre d'e-mails que vous envoyez via vos adresses IP dédiées sur la base d'un plan de préparation prédéfini. La quantité quotidienne maximale de courrier augmente dès le premier jour pour atteindre un maximum de 50 000 e-mails en 45 jours. Cette augmentation progressive permet à vos adresses IP de se forger une réputation positive auprès des fournisseurs de services Internet (FSI).

Les étapes suivies au cours de la procédure de préparation automatique varient selon que vous possédiez ou non déjà des adresses IP dédiées.

- Lorsque vous demandez des adresses IP dédiées (standard) pour la première fois, SES répartit vos envois d'e-mails entre vos adresses IP dédiées et un ensemble d'adresses qui sont partagées avec d'autres clients SES. SES augmente progressivement le nombre de messages envoyés à partir de vos adresses IP dédiées.
- Si vous possédez déjà des adresses IP dédiées, SES répartit vos envois d'e-mail entre vos adresses IP dédiées existantes (qui sont déjà préparées) et vos nouvelles adresses IP dédiées (qui ne sont pas préparées). SES augmente progressivement le nombre de messages envoyés à partir de vos nouvelles adresses IP dédiées.

> **Note**
>
> La préparation automatique des adresses IP est un processus temporel. Le pourcentage de préparation augmente régulièrement sur 45 jours, indépendamment de votre volume d'envoi.

Une fois que vous avez préparé une adresse IP dédiée, vous devez envoyer autour de 1 000 e-mails par jour à chaque fournisseur de messagerie avec lequel vous souhaitez conserver une réputation positive. Vous devez effectuer cette tâche sur chaque adresse IP dédiée que vous utilisez avec SES.

Vous devez éviter d'envoyer de grands volumes de courrier immédiatement après la fin du processus de préparation. Augmentez plutôt lentement le nombre d'e-mails que vous envoyez jusqu'à ce que vous atteigniez votre volume cible. Si un fournisseur de messagerie détecte une augmentation importante soudaine du nombre d'e-mails envoyés à partir d'une adresse IP, il risque de bloquer ou de limiter la remise des messages provenant de cette adresse.

Désactivation du processus de préparation automatique sur les adresses IP dédiées (standard)

Lorsque vous achetez de nouvelles adresses IP dédiées standard, Amazon SES les prépare automatiquement pour vous, car la fonction de préparation automatique des adresses IP est activée par défaut pour votre compte. Si vous préférez préparer vous-même les adresses IP dédiées, vous pouvez désactiver la fonction de préparation automatique au niveau du compte pour toutes vos adresses IP.

Si vous désactivez la fonction de préparation automatique, toutes les adresses IP dédiées louées ultérieurement sont ajoutées à votre compte avec un statut de préparation Terminé, ce qui les rend utilisables sans qu'elles aient été préparées. Cela signifie que vous êtes responsable de veiller à ce

que ces adresses IP soient correctement préparées avant de les utiliser pour des envois réguliers. Toute adresse IP en cours de préparation au moment où vous désactivez la fonction de préparation automatique n'est pas affectée.

> **Important**
>
> Si vous désactivez la fonction de préparation automatique, il vous incombe de préparer des adresses IP dédiées vous-même. Si vous envoyez des e-mails à partir d'adresses qui n'ont pas été préparées, vous risquez de connaître de mauvais taux de remise.

Pour désactiver (ou réactiver) la fonction de préparation automatique pour toutes les adresses IP dédiées (standard) dans votre compte

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation de gauche, choisissez Dedicated IPs (Adresses IP dédiées).
3. Sélectionnez l'onglet Standard IP pools (Groupes d'adresses IP standard) sur la page Dedicated IPs (Adresses IP dédiées).
4. Choisissez Disable auto warm-up (Désactiver la préparation automatique) dans le panneau Standard overview (Présentation standard) pour désactiver la préparation automatique, ou choisissez Enable auto warm-up (Activer la préparation automatique) pour réactiver la préparation automatique.

Préparation manuelle des adresses IP dédiées (standard)

Vous pouvez augmenter ou diminuer manuellement le volume d'envoi actuel de vos adresses IP dédiées (standard) en modifiant leur pourcentage de préparation, arrêter prématurément le processus de préparation, régler le volume d'envoi actuel à 0 % et relancer le processus de préparation.

Pour préparer manuellement les adresses IP dédiées (standard)

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation de gauche, choisissez Dedicated IPs (Adresses IP dédiées).
3. Sélectionnez l'onglet Standard IP pools (Groupes d'adresses IP standard) sur la page Dedicated IPs (Adresses IP dédiées).

4. Dans le panneau All Standard dedicated IPs (Toutes les adresses IP dédiées standard), sélectionnez une adresse IP, choisissez Edit warm up (Modifier la préparation) et sélectionnez l'une des options suivantes :

   a. Edit percentage (Modifier le pourcentage) : saisissez une valeur dans le champ Warm-up percentage (Pourcentage de préparation) pour augmenter ou diminuer le volume d'envoi actuel de votre adresse IP en modifiant son pourcentage de préparation, puis sélectionnez Save changes (Enregistrer les modifications).

      La colonne Warm-up status (Statut de préparation) indique `In progress` et la colonne Warm-up percentage (Pourcentage de préparation) affiche la valeur que vous avez saisie.

   b. Mark as Complete (Marquer comme terminé) : lisez la section Mark warm-up as Complete? (Marquer la préparation comme étant terminée ?) pour confirmer que vous comprenez bien les implications de l'arrêt prématuré du processus de préparation automatique, puis choisissez Mark as Complete (Marquer comme terminé).

      La colonne Warm-up status (Statut de préparation) indique `Complete` et la colonne Warm-up percentage (Pourcentage de préparation) affiche `100%`.

   c. Reset percentage (Réinitialiser le pourcentage) : lisez la section Reset warm-up percentage? (Réinitialiser le pourcentage de préparation ?) pour confirmer que vous réglez le volume d'envoi actuel de l'adresse IP à 0 % et que vous devrez redémarrer le processus de préparation automatique ou définir manuellement le pourcentage de préparation, puis choisissez Reset (Réinitialiser).

      La colonne Warm-up status (Statut de préparation) indique `In progress` et la colonne Warm-up percentage (Pourcentage de préparation) affiche `0%`.

Création de groupes d'adresses IP dédiées standard pour des adresses IP dédiées (standard)

Si vous avez acheté plusieurs adresses IP dédiées (standard) à utiliser avec Amazon SES, vous pouvez créer des groupes de ces adresses, appelés groupes d'adresses IP dédiées. Le regroupement d'adresses IP dédiées (standard) au sein d'un groupe facilite leur gestion. Un scénario courant consiste à créer un groupe pour l'envoi de communications marketing et un autre pour l'envoi d'e-mails transactionnels. Votre réputation d'expéditeur pour les e-mails transactionnels est

ainsi isolée de vos e-mails marketing. Dans ce scénario, si une campagne marketing génère de nombreuses réclamations, cela n'a pas d'impact sur la remise de vos e-mails transactionnels.

Cette section contient des procédures pour la création de groupes d'adresses IP dédiées.

> **Note**
>
> Vous pouvez également créer des jeux de configuration qui utilisent un groupe d'adresses IP partagées par tous les clients SES. Le groupe d'adresses IP partagées est utile lorsque vous avez besoin d'envoyer un e-mail qui n'est pas en adéquation avec vos comportements d'envoi habituels. Pour en savoir plus sur l'utilisation du groupe d'adresses IP partagées avec un jeu de configurations, consultez Attribuer des groupes d'adresses IP dans Amazon SES.

Pour créer un groupe d'adresses IP dédié aux adresses IP dédiées (standard) à l'aide de la console SES

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES sur la page https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation de gauche, choisissez Dedicated IPs (Adresses IP dédiées).

   > **Note**
   >
   > Si vous ne disposez actuellement d'aucune adresse IP dédiée (standard) sur votre compte, la page d'intégration Dedicated IPs (Adresses IP dédiées) s'affiche, vous donnant la possibilité d'acheter des adresses IP dédiées (standard). Pour de plus amples informations, veuillez consulter the section called “Demande d'adresses IP dédiées (standard)”.

3. Sélectionnez l'onglet Standard IP pools (Groupes d'adresses IP standard) sur la page Dedicated IPs (Adresses IP dédiées).
4. Dans le volet All Dedicated IP (standard) pools (Tous les groupes d'adresses IP dédiées (standard)), choisissez Create Standard IP pool (Créer un groupe d'adresses IP standard).

   La page Create IP Pool (Créer un groupe d'adresses IP) s'ouvre.
5. Dans le panneau Pool details (Détails du groupe),

a. Choisissez Standard (self managed) (Standard (autogéré)) dans le champ Scaling mode (Mode de mise à l'échelle).

b. Saisissez un nom pour votre groupe d'adresses IP dans le champ IP pool name (Nom du groupe d'adresses IP).

> **Note**
>
> Le nom du groupe d'adresses IP doit être unique et ne peut pas être un doublon d'un nom de groupe d'adresses IP gérées dans votre compte.

c. (Facultatif) Si vous souhaitez ajouter des adresses IP dédiées standard existantes à ce groupe d'adresses IP, sélectionnez-les dans la liste déroulante du champ Dedicated IP addresses (Adresses IP dédiées).

> **Note**
>
> Si vous sélectionnez une adresse IP déjà associée à un groupe d'adresses IP, elle sera désormais associée uniquement à ce groupe d'adresses IP.

6. (Facultatif) Vous pouvez associer ce groupe d'adresses IP à un jeu de configuration en sélectionnant ce dernier dans la liste déroulante du champ Configuration sets (Jeux de configuration).

> **Note**
>
> - Si vous sélectionnez un jeu de configuration déjà associé à un groupe d'adresses IP, il sera désormais associé uniquement à ce groupe d'adresses IP.
> - Pour ajouter ou supprimer des jeux de configuration associés après la création de ce groupe d'adresses IP, modifiez le paramètre Sending IP pool (Groupe d'adresses IP d'envoi) de ce jeu de configuration.
> - Si vous n'avez pas encore créé de jeux de configuration, consultez Jeux de configurations.

7. (Facultatif) Vous pouvez ajouter une ou plusieurs balises à ce groupe d'adresses IP en incluant une clé de balise et une valeur facultative pour cette clé.

a. Choisissez Add new tag (Ajouter une nouvelle balise) et entrez la Clé. Vous pouvez aussi ajouter une valeur pour la balise.

b. Pour ajouter la balise, sélectionnez Enregistrer les modifications.

   Vous pouvez ajouter jusqu'à 50 balises. Vous pouvez supprimer une balise en choisissant Remove (Supprimer).

8. Sélectionnez Create pool (Créer un groupe).

> **Note**
>
> Une fois que vous avez créé un groupe d'adresses IP standard, vous avez la possibilité de le transformer en un groupe d'adresses IP géré. Consultez Création d'un groupe d'adresses IP gérées.

Adresses IP dédiées (gérées) pour Amazon SES

Les adresses IP dédiées (gérées) sont une fonctionnalité d'Amazon SES qui configure et gère automatiquement les adresses IP dédiées en votre nom afin de vous permettre de commencer rapidement et facilement à utiliser des adresses IP dédiées gérées par SES. Cela contribue à garantir que vos adresses IP dédiées seront utilisées de manière efficace et optimale pour la manière dont vous envoyez des e-mails.

Pour activer des adresses IP dédiées (gérées) dans votre compte, créez un groupe d'adresses IP gérées et SES s'occupe du reste. SES déterminera le nombre d'adresses IP dédiées dont vous avez besoin en fonction de vos modèles d'envoi, les créera pour vous, puis gérera leur mise à l'échelle en fonction de vos exigences d'envoi.

Une fois activées, vous pouvez utiliser des adresses IP dédiées (gérées) dans l'envoi de vos e-mails en associant le groupe d'adresses IP gérées à un jeu de configurations, puis en spécifiant ce dernier lors de l'envoi d'e-mails. Le jeu de configuration peut également être appliqué à une identité d'envoi à l'aide d'un jeu de configuration par défaut.

Avantages et fonctionnalités des adresses IP dédiées (gérées)

Les adresses IP dédiées que vous créez avec des adresses IP dédiées (gérées) automatisent les tâches de gestion afin de garantir que vos adresses IP dédiées seront utilisées de manière optimale en fonction de la manière dont vous envoyez des e-mails :

- Intégration aisée : pour bien démarrer avec les adresses IP dédiées (gérées), vous créez un groupe d'adresses IP gérées directement dans la console SES. Les adresses IP dédiées sont automatiquement allouées au groupe. Vous pouvez commencer à envoyer avec le pool d'adresses IP géré sans avoir à ouvrir un dossier de demande via le AWS Support Center.
- Dimensionnement automatique par fournisseur de services Internet : vous n'avez pas besoin de surveiller ou de dimensionner manuellement vos pools d'adresses IP dédiés, car le pool d'adresses IP géré évolue automatiquement en fonction de l'utilisation. Il prend également en compte les politiques spécifiques des FSI. Par exemple, si SES détecte qu'un FSI prend en charge un faible quota d'envoi quotidien, le groupe monte en puissance pour mieux répartir le trafic vers ce FSI sur un plus grand nombre d'adresses IP.
- Préparation intelligente : les adresses IP dédiées (gérées) commencent à envoyer du courrier aux FSI en fonction de leur capacité. C'est-à-dire, selon leur taux de préparation actuel. Elles suivent automatiquement le niveau de préparation pour chaque FSI individuellement. En outre, la fonctionnalité d'adresses IP dédiées (gérées) fournit des informations sur votre réputation à un taux quotidien effectif auprès des meilleurs fournisseurs de services Internet sous la forme de CloudWatch statistiques Amazon et de tableaux de bord intégrés.
  - Préparation par FSI : SES suit la réputation de chaque adresse IP dans le groupe d'adresses IP gérées pour chaque FSI individuellement. Par exemple, si vous envoyez tout votre trafic vers Gmail, les adresses IP sont considérées comme préparées uniquement pour Gmail et non préparées pour les autres FSI. Si vous modifiez votre modèle de trafic en augmentant le nombre d'e-mails envoyés à Hotmail, SES augmente lentement le trafic pour Hotmail, car les adresses IP ne sont pas encore préparées.
  - Échauffement adaptatif et transition vers le pool partagé — Le réglage de l'échauffement est adaptatif et prend en compte les modèles d'envoi réels. Lorsque le volume d'envoi vers un FSI baisse, le pourcentage de préparation baisse également pour ce FSI. Au début de la phase de préchauffage, tout envoi excessif par rapport au niveau actuel de préchauffage est envoyé via les adresses IP partagées avec d'autres utilisateurs d'Amazon SES : le pool partagé SES. Dans les phases ultérieures de la préparation, tout envoi excessif est ralenti de manière proactive et réessayé plus tard.

    > **Important**
    >
    > Alors que les adresses IP dédiées (gérées) réchauffent automatiquement vos adresses IP dédiées, une partie de ce processus automatique consiste à travailler de manière interactive avec le pool d'adresses IP partagé de SES.

- Si votre taux d'envoi est trop élevé pour vos nouvelles adresses IP dédiées pendant leur préchauffage, SES répartira automatiquement une partie de vos envois dans le pool d'adresses IP partagées de SES afin de protéger la réputation de vos nouvelles adresses IP dédiées.
- Même une fois que vos nouvelles adresses IP dédiées sont complètement réchauffées, il n'est pas garanti que tous vos envois passeront par elles 100 % du temps. Par exemple, si votre taux d'envoi augmente soudainement et que les adresses IP dédiées (gérées) déterminent qu'il doit allouer une adresse IP dédiée supplémentaire, cela lancera le processus de préchauffage qui inclut l'utilisation du pool partagé. De même, si votre taux d'envoi chute soudainement très bas, tous vos envois pourraient passer au pool IP partagé de SES, voirthe section called "Importance de la préparation".

- Demande et restitution automatiques d'adresses IP dédiées : vous n'avez pas besoin de demander ou de céder des adresses IP dédiées gérées par le biais du AWS Support Center, comme c'est le cas lorsque vous utilisez des adresses IP dédiées (standard). Lors d'une intégration avec des adresses IP dédiées (gérées) directement depuis la console, l'interface CLI ou l'API SES, les adresses IP dédiées vous sont automatiquement allouées et des frais vous sont facturés en fonction du volume de messages que vous envoyez. Lorsque vous supprimez un groupe d'adresses IP créé par des adresses IP dédiées (gérées) ou que vous vous désactivez des adresses IP dédiées (gérées), les adresses IP qui vous sont allouées sont automatiquement abandonnées et les frais cessent immédiatement.
  - Getting your first dedicated IP address (Obtenir votre première adresse IP dédiée : la fonction d'adresses IP dédiées (gérées) vous attribuera automatiquement votre première adresse IP dédiée dès que votre volume d'envoi atteindra des centaines d'e-mails sur une période de quelques jours. Ainsi, l'adresse IP à partir de laquelle vous effectuez vos envois peut se forger une réputation d'expéditeur et améliorer la livraison de vos messages. (Si vous ne prévoyez pas que votre volume d'envoi atteigne ce niveau, vous devriez utiliser des adresses IP partagées. Consultez le tableau comparatif dans Adresses IP dédiées pour examiner le type d'adresses IP qui conviennent le mieux à votre mode d'envoi d'e-mail).

Pourquoi une bonne préparation des adresses IP est importante

Pour que votre e-mail soit livré par votre adresse IP dédiée, celle-ci doit avoir une bonne réputation auprès du fournisseur d'accès Internet destinataire. Les FAI n'accepteront qu'un faible volume d'e-mails provenant d'une IP qu'ils ne reconnaissent pas. Lorsqu'une adresse IP vous est affectée pour

la première fois, elle est nouvelle et ne sera pas reconnue par le fournisseur d'accès à Internet destinataire, car elle n'a pas de réputation associée. Pour que la réputation d'une adresse IP soit établie, elle doit progressivement établir une relation de confiance avec le FAI destinataire ; ce processus d'établissement progressif de la confiance est appelé préparation. Immédiatement après que les adresses IP dédiées (gérées) aient alloué un IP, elles lancent le processus de préparation intelligente.

Grâce aux fonctions Warmup per ISP (Préparation par ISP) et Adaptive warmup (Préparation adaptative) des IP dédiées (gérées), la continuité des activités est maintenue tout au long du cycle de préparation en garantissant la livraison de vos e-mails. Une fois la phase de préparation terminée, toute capacité excédentaire est mise en file d'attente et envoyée uniquement par le groupe d'adresses IP dédié. Toutefois, si vous avez une adresse IP dédiée et que le volume de vos envois est inférieur au volume minimum requis pour préserver la réputation IP, les adresses IP dédiées (gérées) peuvent supprimer votre adresse IP dédiée et vos envois seront acheminés via le pool d'adresses IP partagé de SES.

> **Note**
>
> Si vous envoyez de petits volumes d'e-mail (moins de quelques centaines par jour en l'espace de quelques jours), il serait plus avantageux de passer par le groupe d'IP partagées de SES. Pour savoir si les IP dédiées (gérées) conviennent à votre mode d'envoi d'e-mail, consultez le tableau comparatif dans Adresses IP dédiées.

Création d'un groupe d'adresses IP gérées pour activer des adresses IP dédiées (gérées)

Pour activer les adresses IP dédiées (gérées), vous devez d'abord créer un groupe d'adresses IP géré. Une fois que vous avez créé un groupe géré, la fonction détermine le nombre d'adresses IP dont vous avez besoin en fonction de vos modèles d'envoi et s'adapte de manière dynamique à vos besoins.

Pour utiliser votre groupe géré pour envoyer des e-mails, vous devez associer le groupe géré à un jeu de configurations, puis spécifier ce dernier lors de l'envoi d'e-mails. Le jeu de configuration peut également être appliqué à une identité d'envoi à l'aide d'un jeu de configuration par défaut.

Il existe deux façons de créer un groupe d'adresses IP géré :

- Créez un nouveau groupe.

- Transformez un groupe existant standard en un groupe géré.

Vous trouverez dans les procédures suivantes des instructions pour chacune des deux méthodes.

Pour créer un groupe ou transformer un groupe en un groupe d'adresses IP géré en utilisant la console SES

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation de gauche, choisissez Dedicated IPs (Adresses IP dédiées).
3. Selon que vous souhaitez créer un nouveau groupe d'adresses IP géré ou transformer un groupe d'adresses IP dédiées standard en un groupe géré, suivez les instructions correspondantes :

   Create new pool

   Pour créer un groupe d'adresses IP géré

   1. Effectuez l'une des actions suivantes :

      a. S'il n'existe pas d'adresses IP dédiées dans votre compte :

         - La page d'intégration Adresses IP dédiées s'affiche. Dans le volet Présentation des adresses IP dédiées (gérées), choisissez Activer les adresses IP dédiées.

           La page Create IP Pool (Créer un groupe d'adresses IP) s'ouvre.

      b. Si vous avez des adresses IP dédiées existantes sur votre compte :

         i. Sélectionnez l'onglet Managed IP pools (Groupes d'adresses IP gérées) sur la page Dedicated IPs (Adresses IP dédiées).

         ii. Dans le volet All Dedicated IP (managed) pools (Tous les groupes d'adresses IP dédiées gérées), choisissez Create Managed IP pool (Créer un groupe d'adresses IP gérées).

             La page Create IP Pool (Créer un groupe d'adresses IP) s'ouvre.

   2. Dans le panneau Pool details (Détails du groupe),

      a. Choisissez Managed (auto managed) (Géré (gestion automatique)) dans le champ Scaling mode (Mode de mise à l'échelle).

b. Saisissez un nom pour votre groupe géré dans le champ IP pool name (Nom du groupe d'adresses IP).

> **Note**
>
> - Le nom du groupe d'adresses IP doit être unique. Il ne peut pas s'agir d'un doublon d'un nom de groupe d'adresses IP dédiées standard dans votre compte.
> - Il ne peut pas exister plus de 50 groupes d'adresses IP dédiées par Région AWS dans votre compte, qu'il s'agisse de groupes d'adresses IP gérés ou standard.

3. (Facultatif) Vous pouvez associer ce groupe d'adresses IP gérées à un jeu de configuration en choisissant ce dernier dans la liste déroulante du champ Configuration sets (Jeux de configuration).

> **Note**
>
> - Si vous choisissez un jeu de configuration déjà associé à un groupe d'adresses IP, il sera associé à ce groupe géré et ne sera plus associé au groupe précédent.
> - Pour ajouter ou supprimer des jeux de configuration associés après la création de ce groupe géré, modifiez le paramètre Sending IP pool (Groupe d'adresses IP d'envoi) de ce jeu de configuration dans le panneau General details (Informations générales).
> - Si vous n'avez pas encore créé de jeux de configuration, consultez Jeux de configurations.

4. (Facultatif) Vous pouvez ajouter une ou plusieurs balises à votre groupe d'adresses IP en incluant une clé de balise et une valeur facultative pour la clé.

   a. Choisissez Add new tag (Ajouter une nouvelle balise) et entrez la Clé. Vous pouvez aussi ajouter une valeur pour la balise. Vous pouvez ajouter jusqu'à 50 balises. Si vous faites une erreur, choisissez Remove (Supprimer).

   b. Pour ajouter les balises, sélectionnez Save changes (Enregistrer les modifications).

Une fois que vous avez créé le groupe, vous pouvez ajouter, supprimer ou modifier des balises en sélectionnant le groupe géré et en choisissant Edit (Modifier).

5. Sélectionnez Create pool (Créer un groupe).

> **Note**
>
> - Une fois que vous avez créé un groupe d'adresses IP gérées, il ne peut pas être converti en groupe d'adresses IP standard.
> - Lorsque vous utilisez des adresses IP dédiées (gérées), vous ne pouvez pas avoir plus de 10 000 identités d'envoi (domaines et adresses e-mail, toutes combinaisons Région AWS confondues) par compte.

Convert standard to managed

Pour convertir un groupe d'adresses IP dédiées standard en groupe géré

1. Sélectionnez l'onglet Standard IP pools (Groupes d'adresses IP standard) sur la page Dedicated IPs (Adresses IP dédiées).
2. Dans le panneau Tous les groupes d'adresses IP dédiées (standard), cochez la case correspondant au groupe d'adresses IP dédiées que vous voulez faire passer de standard à géré.
3. Choisissez Convertir en groupe géré (lisez le contenu de la boîte de dialogue Convertir en groupe d'adresses IP géré pour vérifier que vous avez bien compris les conditions de conversion de votre groupe d'adresses IP dédiées standard en groupe géré).

> **Note**
>
> Avant de faire passer le type de votre groupe d'adresses IP dédiées de standard à géré, tenez compte des points suivants :
>
> 1. Toutes vos adresses IP dédiées actuelles (standard) seront déplacées dans le groupe géré.
> 2. Si vous louez actuellement trop d'adresses IP dédiées (standard) pour votre volume d'envois, les adresses IP redondantes seront supprimées dans le groupe d'adresses IP dédiées (géré).

3. Si certaines de vos adresses IP dédiées (groupe standard) font partie d'une liste d'adresses autorisées pour d'autres applications, vous ne devez pas les transférer vers le groupe géré, car elles seront supprimées si elles deviennent redondantes (reportez-vous au point n° 2).
4. Vous ne serez plus facturé par adresse IP, mais en fonction du volume que vous envoyez par l'intermédiaire du groupe géré. Consultez Tarification Amazon SES.

4. Si vous acceptez les conditions énoncées, choisissez Confirmer. Une bannière s'affiche pour confirmer que votre groupe d'adresses IP dédiées standard a été converti en groupe géré.

> **Note**
>
> Les jeux de configurations ou les identifications que vous aviez associés au groupe standard avant la conversion sont maintenant associés au groupe géré, ce qui permet une transition fluide pour les envois d'e-mails utilisant le jeu de configurations.

La publication d'événements permet de suivre les performances d'envoi du groupe géré. Pour plus d'informations, consultez the section called “Surveillance de l'envoi d'e-mails à l'aide de la publication d'événements”.

Consultation des métriques d'envoi et de capacité du groupe d'adresses IP géré dans la console Amazon SES

Pour les groupes d'adresses IP gérés que vous avez créés, la console SES vous permet d'observer facilement de quelle manière ils sont utilisés pour vos envois d'e-mails grâce à des cartes et des graphiques chronologiques qui présentent les métriques d'envoi ainsi que l'utilisation et la capacité du fournisseur de services Internet.

Pour consulter les métriques d'envoi et de capacité du groupe d'adresses IP géré à l'aide de la console SES

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.

2. Dans le panneau de navigation de gauche, choisissez Dedicated IPs (Adresses IP dédiées).
3. Sélectionnez l'onglet Managed IP pools (Groupes d'adresses IP gérées) sur la page Dedicated IPs (Adresses IP dédiées).
4. Selon que vous souhaitez consulter les statistiques d'envoi et de capacité dans la console Amazon SES ou dans la CloudWatch console Amazon, suivez les instructions correspondantes :

   Amazon SES console

   Pour consulter les métriques d'envoi et de capacité dans la console Amazon SES

   1. Dans le tableau Tous les groupes d'adresses IP dédiées (gérés), sélectionnez le nom d'un groupe d'adresses IP géré figurant dans la colonne Groupe d'adresses IP pour en afficher les détails.

      La page d'informations sur le groupe d'adresses IP sélectionné s'ouvre avec les cartes et les graphiques chronologiques suivants :

      a. Cartes :

         - Statut d'envoi – Indique si le volume et la fréquence de vos envois sont suffisants pour utiliser des adresses IP dédiées en affichant l'un des deux états suivants :
           - Volume insuffisant – Votre volume d'envois est trop faible.
           - Envoi via des adresses IP dédiées – Une ou plusieurs adresses IP dédiées sont utilisées dans votre groupe géré.
         - Volume d'envoi d'adresses IP dédiées gérées – Volume d'e-mails envoyés via des adresses IP dédiées dans votre groupe géré au cours des 7 derniers jours.
         - Pourcentage d'envoi d'adresses IP dédiées gérées – Pourcentage d'e-mails envoyés via des adresses IP dédiées dans votre groupe géré au cours des 7 derniers jours.

      b. Graphiques :

         - Volume envoyé : volume d'e-mails envoyés au cours des 7 derniers jours via des adresses IP dédiées gérées par rapport aux adresses IP partagées.
         - Pourcentage du volume d'envoi : pourcentage d'e-mails envoyés au cours des 7 derniers jours via des adresses IP dédiées gérées par rapport aux adresses IP partagées.

- Capacité des ISP – Affiche la quantité d'e-mails envoyés via des adresses IP dédiées de votre groupe géré par fournisseur de services Internet parmi les 10 les plus utilisés, ainsi que leur capacité disponible au cours de l'envoi :
  - Envoie pour l'ISP (barres rouges) – Volume d'e-mails que vous avez envoyé au cours des dernières 24 heures via le fournisseur de services Internet sélectionné.
  - Capacité pour les IPS (ligne bleue) – Capacité disponible du fournisseur de services Internet sélectionné au cours des dernières 24 heures.

2. Pour filtrer en fonction d'un fournisseur de services Internet spécifique pour le graphique Capacité des ISP, choisissez la zone de liste ISP et sélectionnez un fournisseur de services Internet. Le graphique est alors mis à jour avec les métriques de l'ISP sélectionné. (Si vous ne filtrez pas en fonction d'un ISP, Gmail s'affiche par défaut).

Amazon CloudWatch console

Pour consulter les statistiques d'envoi et de capacité dans la CloudWatch console Amazon

- Dans le tableau Tous les pools d'adresses IP dédiés (gérés), sélectionnez le <pool_name>lien Voir CloudWatch les métriques dans la colonne CloudWatchdes métriques pour en afficher les détails.

  La page du pool d'adresses IP sélectionné s'ouvre dans la CloudWatch console et affiche les statistiques suivantes :

  - Send – Volume d'e-mails envoyé via les adresses IP dédiées gérées et les adresses IP partagées.
  - ApproximateDedicatedSendingPercentage— Indique le pourcentage approximatif du trafic diffusé via une adresse IP dédiée.
  - SentLast24 heures — Le volume d'e-mails que vous avez envoyés au cours des dernières 24 heures via le fournisseur de services Internet sélectionné. (Libellé Envoie pour l'ISP dans la console SES.)
  - Available24 HourSend — La capacité disponible du FAI sélectionné au cours des dernières 24 heures. (Libellé Capacité pour les ISP dans la console SES.)

Suppression d'un groupe d'adresses IP géré et désactivation des adresses IP dédiées (géré)

Lorsque vous supprimez un groupe d'adresses IP gérées, toutes les adresses IP qui lui ont été attribuées sont automatiquement abandonnées. Si vous ne possédez qu'un seul groupe d'adresses IP gérées et que vous le supprimez, ou si vous supprimez le dernier groupe d'adresses IP gérées restant, vous vous désabonnerez de la fonction d'adresses IP dédiées (gérées) et vous ne serez plus facturé.

Pour supprimer un groupe d'adresses IP gérées à l'aide de la console SES

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation de gauche, choisissez Dedicated IPs (Adresses IP dédiées).
3. Sélectionnez l'onglet Managed IP pools (Groupes d'adresses IP gérées) sur la page Dedicated IPs (Adresses IP dédiées).
4. Dans le tableau All Dedicated IP (managed) pools (Tous les groupes d'adresses IP dédiées (gérées)), sélectionnez la case d'option à côté du nom IP pool (Groupe d'adresses IP) du groupe géré que vous souhaitez supprimer et choisissez Delete (Supprimer).
5. Dans la fenêtre contextuelle, vous aurez la possibilité de confirmer votre choix en sélectionnant Delete (Supprimer) ou Cancel (Annuler) pour conserver votre groupe géré.

> **Note**
>
> Si vous n'avez qu'un seul groupe géré ou si vous supprimez votre dernier groupe géré, la fenêtre contextuelle vous rappellera qu'en supprimant le groupe géré restant, vous vous désabonnerez de la fonction d'adresses IP dédiées (gérées) et que vous ne serez plus facturé. Vous devrez saisir `Disable` dans le champ de confirmation avant de pouvoir choisir Delete (Supprimer).

Utilisation de vos propres adresses IP pour envoyer des e-mails à l'aide d'Amazon SES

Amazon SES inclut une fonction appelée Bring Your Own IP (BYOIP, ou Adresse IP à fournir), qui permet d'utiliser vos propres adresses IP pour envoyer des e-mails via Amazon SES. Si vous utilisez

déjà une plage d'adresses IP pour envoyer des e-mails, vous pouvez demander à rendre votre plage d'adresses IP disponible pour l'envoi d'e-mails via Amazon SES.

> **Note**
>
> La fonctionnalité BYOIP est disponible uniquement pour les adresses IP dédiées que vous configurez manuellement ; elle ne peut pas être utilisée avec des adresses IP dédiées (gérées).

Par exemple, BYOIP est utile lorsque vous avez développé une réputation IP positive à l'aide d'un système interne d'envoi d'e-mails, mais que vous souhaitez migrer vers Amazon SES. En utilisant BYOIP, vous pouvez commencer à envoyer des e-mails via Amazon SES immédiatement, sans avoir à rétablir la réputation de vos adresses IP.

Prérequis

Pour utiliser BYOIP, votre plage d'adresses IP doit répondre aux exigences suivantes :

- La plage d'adresses doit être enregistrée auprès de votre registre Internet régional (RIR), tel que l'ARIN (American Registry for Internet Numbers), le RIPE NCC (Réseaux IP Européens Network Coordination Centre) ou l'APNIC (Asia-Pacific Network Information Centre). La plage d'adresses doit être enregistrée auprès d'une entreprise ou d'une entité institutionnelle et ne peut pas être enregistrée auprès d'une personne.
- Vous devez être en mesure de fournir la preuve que vous possédez la plage d'adresses en envoyant un message d'autorisation signé.
- L'historique des adresses de la plage d'adresses IP doit être propre. Nous pouvons enquêter sur la réputation de la plage d'adresses IP et nous réservons le droit de rejeter une plage d'adresses IP si elle contient des adresses IP ayant une mauvaise réputation ou étant associées à un comportement malveillant.
- La plage d'adresses IP ne peut pas inclure de plages d'adresses IP qui ont été introduites dans un autre Service AWS pour BYOIP, tel qu'Amazon EC2.

Considérations

Plusieurs facteurs doivent être pris en compte avant de demander le transfert de vos plages d'adresses IP vers Amazon SES :

- La plage d'adresses la plus spécifique que vous pouvez spécifier est /24. En d'autres termes, si vous transférez la plage IP 203.0.113.0/24 vers votre compte Amazon SES, vous pouvez envoyer à partir d'un total de 256 adresses, allant de 203.0.113.0 à 203.0.113.255. Vous devez transférer l'ensemble de la plage. Amazon SES ne vous permet pas actuellement de transférer des adresses IP individuelles.
- Si vous utilisez BYOIP pour une plage spécifique d'adresses IP, vous ne pouvez accéder à cette plage qu'à partir d'une seule région Région AWS.
- Vous pouvez importer cinq plages d'adresses par région dans votre Compte AWS.
- Si vous utilisez vos propres adresses IP, vous ne pouvez pas utiliser les adresses dans le groupe d'adresses IP Amazon SES partagées. Si vous devez utiliser ces adresses IP partagées, vous pouvez utiliser Amazon SES dans une autre Région AWS ou créer un Compte AWS.
- Il y a des frais mensuels pour chaque adresse IP que vous utilisez avec BYOIP. Pour plus d'informations, veuillez consulter Tarification Amazon SES.

Utilisation de vos propres adresses IP avec Amazon SES

Afin d'éviter que nos systèmes ne soient utilisés pour envoyer du contenu non sollicité ou malveillant, nous devons examiner attentivement chaque demande BYOIP.

Si vous souhaitez utiliser votre propre plage IP avec Amazon SES, veuillez envoyer les informations suivantes à ses-byoip-request@amazon.com :

- Votre ID de compte AWS.
- La Région AWS dans laquelle vous souhaitez utiliser la plage d'adresses IP, par ex., ap-south-1.
- Description de votre cas d'utilisation.
- Plage d'adresses IP avec laquelle vous souhaitez utiliser Amazon SES.
- Nom du registre Internet avec lequel la plage est enregistrée.

Nous traiterons votre demande dans un délai de 48 heures ouvrables. Dans nos communications avec vous, nous pouvons demander des informations supplémentaires, y compris des documents prouvant que vous êtes propriétaire de la plage IP.

Virtual Deliverability Manager pour Amazon SES

La délivrabilité, c'est-à-dire la garantie que vos e-mails parviennent dans les boîtes de réception des destinataires plutôt que dans les dossiers de spam ou de courrier indésirable, est un élément essentiel d'une stratégie d'e-mails réussie.

Virtual Deliverability Manager est une fonction Amazon SES qui vous aide à améliorer la délivrabilité des e-mails, notamment en augmentant la délivrabilité dans les boîtes de réception et les conversions d'e-mails, en fournissant des informations sur vos données d'envoi et de livraison et en vous donnant des conseils pour résoudre les problèmes qui affectent négativement votre taux de réussite des livraisons et votre réputation.

Pourquoi la délivrabilité dans votre boîte de réception et la réputation de l'expéditeur sont importantes

La délivrabilité dans la boîte de réception est un facteur clé lorsqu'il s'agit de convertir des e-mails (lorsqu'un destinataire agit après avoir ouvert un e-mail). Les clients qui ne reçoivent pas vos messages ne pourront pas les voir et encore moins interagir avec eux.

La réputation des expéditeurs a la plus grande influence sur la délivrabilité dans les boîtes de réception au niveau de l'expérience client : elle détermine si les messages indésirables parviennent aux destinataires ou si les messages nécessaires sont acheminés vers des dossiers de courrier indésirable ou bloqués avant de pouvoir atteindre les boîtes aux lettres des destinataires.

Comment Virtual Deliverability Manager peut contribuer à améliorer la délivrabilité et la réputation

Virtual Deliverability Manager vous aide à améliorer à la fois votre délivrabilité et votre réputation grâce à un tableau de bord qui offre des vues d'ensemble et détaillées du programme de messagerie de votre compte, afin de vous aider à vous concentrer sur les problèmes éventuels, et à un conseiller qui propose des solutions pour remédier aux problèmes d'infrastructure qui nuisent à la délivrabilité et à la réputation de vos e-mails.

- Tableau de bord : fournit des informations sur vos données de délivrabilité en mettant l'accent sur le compte, le FAI, l'identité d'envoi et les niveaux du jeu de configurations. Il vous permet d'identifier rapidement les domaines problématiques et les tendances, et de détecter les soucis éventuels avant qu'ils ne se transforment en problèmes de délivrabilité plus importants, tels que des refus temporaires (reports) ou des blocages. Ces informations vous aideront également à améliorer votre réputation d'expéditeur en calculant les heures et les dates idéales pour améliorer l'engagement client et les conversions pour vos campagnes par e-mail.

- Conseiller : fournit des recommandations pour améliorer l'envoi de vos e-mails en signalant les problèmes de configuration qui nuisent à la délivrabilité et à la réputation de vos e-mails. Il recommandera des solutions pour résoudre des problèmes spécifiques liés à l'infrastructure de votre domaine d'envoi, à votre espace IP et à vos enregistrements d'authentification, par exemple lorsque les enregistrements SPF, DMARC ou DKIM n'existent pas ou si la longueur d'une clé DKIM est trop courte.

Démarrer avec Virtual Deliverability Manager

Pour commencer à utiliser Virtual Deliverability Manager, un assistant d'intégration dans la console Amazon SES vous expliquera les étapes pour activer Virtual Deliverability Manager pour votre compte. veuillez consulter the section called “Démarrer”.

Rubriques

Démarrer avec Virtual Deliverability Manager

Pour commencer à utiliser Virtual Deliverability Manager avec votre compte, vous devez l'activer à l'aide de l'assistant d'intégration de la console Amazon SES, qui vous permettra de configurer le suivi de l'engagement et la livraison partagée optimisée. Virtual Deliverability Manager utilise le suivi de l'engagement et la livraison partagée optimisée pour surveiller vos envois et vous aider à améliorer votre délivrabilité et votre réputation.

- Suivi de l'engagement : la possibilité de surveiller le comportement d'engagement des destinataires par le biais d'événements d'ouverture et de clic à l'aide d'un pixel de suivi intégré à un lien encapsulé. Lorsqu'il est déclenché, le pixel de suivi fournit un horodatage indiquant à quel moment un message a été ouvert et indique les liens sur lesquels le destinataire a cliqué. Activer cette option modifie vos URL et vos liens pour inclure les encapsuleurs de suivi de l'engagement Amazon SES.
- Livraison partagée optimisée : choisit automatiquement l'adresse IP optimale à utiliser lors de l'envoi d'e-mails, améliorant ainsi la livraison des messages aux destinataires cibles. Cela ne s'applique pas aux adresses IP dédiées.

Bien que le suivi de l'engagement et la livraison partagée optimisée soient activés par défaut dans l'assistant d'intégration, vous avez la possibilité de les désactiver. Nous vous recommandons vivement de garder les deux fonctionnalités activées pour tirer le meilleur parti de Virtual Deliverability Manager.

Démarrer avec Virtual Deliverability Manager à l'aide de la console Amazon SES

La procédure suivante décrit comment démarrer avec Virtual Deliverability Manager à l'aide de la console Amazon SES.

Pour démarrer avec Virtual Deliverability Manager à l'aide de la console Amazon SES

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le volet de navigation de gauche, choisissez Virtual Deliverability Manager.
3. Cliquez sur l'un des boutons Get started with Virtual Deliverability Manager (Démarrer avec Virtual Deliverability Manager) sur la page Virtual Deliverability Manager overview (Présentation de Virtual Deliverability Manager).
4. Sur la page Select Engagement tracking (Sélectionner le suivi de l'engagement), acceptez la valeur par défaut ou choisissez Turn off engagement tracking (Désactiver le suivi de l'engagement), puis Next (Suivant).

   > **Note**
   >
   > Activer le suivi de l'engagement modifie vos URL et vos liens pour inclure des encapsuleurs de suivi des interactions Amazon SES.

5. Sur la page Select Optimized shared delivery (Sélectionner la livraison partagée optimisée), acceptez la valeur par défaut ou choisissez Turn off optimized shared delivery (Désactiver la livraison partagée optimisée), puis Next (Suivant).

   > **Important**
   >
   > La livraison partagée optimisée peut entraîner des retards préemptifs dans l'envoi de vos e-mails afin de protéger votre réputation d'expéditeur. Si une charge de travail critique doit être envoyée sans délai, nous vous recommandons de ne pas activer ce paramètre. Utilisez plutôt des jeux de configurations pour l'envoi et n'activez la livraison partagée

optimisée que pour les jeux de configurations pour lesquels vous pouvez vous permettre des retards.

6. Vérifiez vos choix en matière de suivi de l'engagement et de livraison partagée optimisée sur la page Review and enable (Vérifier et activer). Choisissez Previous (Précédent) si vous souhaitez revenir en arrière et apporter des modifications ; sinon, choisissez Enable Virtual Deliverability Manager (Activer Virtual Deliverability Manager).

   La page Virtual Deliverability Manager settings (Paramètres de Virtual Deliverability Manager) s'ouvre. Le volet Subscription overview (Présentation des abonnements) indique le statut de Virtual Deliverability Manager et le volet Additional settings (Paramètres supplémentaires) indique le statut de Engagement tracking (Suivi de l'engagement) et de Optimized shared delivery (Livraison partagée optimisée).

Une fois que vous avez activé Virtual Deliverability Manager pour votre compte, vous pouvez définir des paramètres personnalisés indiquant comment un jeu de configurations utilisera le suivi de l'engagement et la livraison partagée optimisée en remplaçant leur définition dans Virtual Deliverability Manager. Cela vous donne la possibilité d'adapter l'envoi de vos e-mails pour des campagnes d'e-mails spécifiques. Par exemple, vous pouvez activer le suivi de l'engagement et la livraison partagée optimisée pour vos e-mails marketing et les désactiver pour vos e-mails transactionnels. Consultez Virtual Deliverability Manager options (Options de Virtual Deliverability Manager) lors de la création ou de la modification d'un jeu de configurations.

Démarrer avec Virtual Deliverability Manager à l'aide de l'AWS CLI

Les exemples suivants décrivent comment démarrer avec Virtual Deliverability Manager à l'aide de l'AWS CLI.

Pour démarrer avec Virtual Deliverability Manager à l'aide de l'AWS CLI

Vous pouvez utiliser l'opération `PutAccountVdmAttributes` dans l'API Amazon SES v2 pour démarrer avec Virtual Deliverability Manager. Vous pouvez appeler cette opération depuis l'AWS CLI, comme illustré dans les exemples suivants.

- Activez Virtual Deliverability Manager sur votre compte :

```
aws --region us-east-1 sesv2 put-account-vdm-attributes --vdm-attributes
 VdmEnabled=ENABLED
```

- Activez à la fois le suivi de l'engagement et la livraison partagée optimisée à l'aide d'un fichier d'entrée :

```
aws --region us-east-1 sesv2 put-account-vdm-attributes --cli-input-json file://
attributes.json
```

Le fichier d'entrée ressemble à ceci :

```
{
    "VdmAttributes": {
        "VdmEnabled": "ENABLED",
        "DashboardAttributes": {
            "EngagementMetrics": "ENABLED"
        },
        "GuardianAttributes": {
            "OptimizedSharedDelivery": "ENABLED"
        }
    }
}
```

Les valeurs des paramètres et les types de données associés peuvent être trouvés en établissant un lien à partir du type de données `VdmAttributes` figurant dans la référence de l'API Amazon SES v2.

> **Note**
>
> Activer le suivi de l'engagement modifie vos URL et vos liens pour inclure des encapsuleurs de suivi des interactions Amazon SES.

> **Important**
>
> La livraison partagée optimisée peut entraîner des retards préemptifs dans l'envoi de vos e-mails afin de protéger votre réputation d'expéditeur. Si une charge de travail critique doit être envoyée sans délai, nous vous recommandons de ne pas activer ce paramètre. Utilisez plutôt des jeux de configurations pour l'envoi et n'activez la livraison partagée optimisée que pour les jeux de configurations pour lesquels vous pouvez vous permettre des retards.

- Pour vérifier le résultat :

```
aws --region us-east-1 sesv2 get-account
```

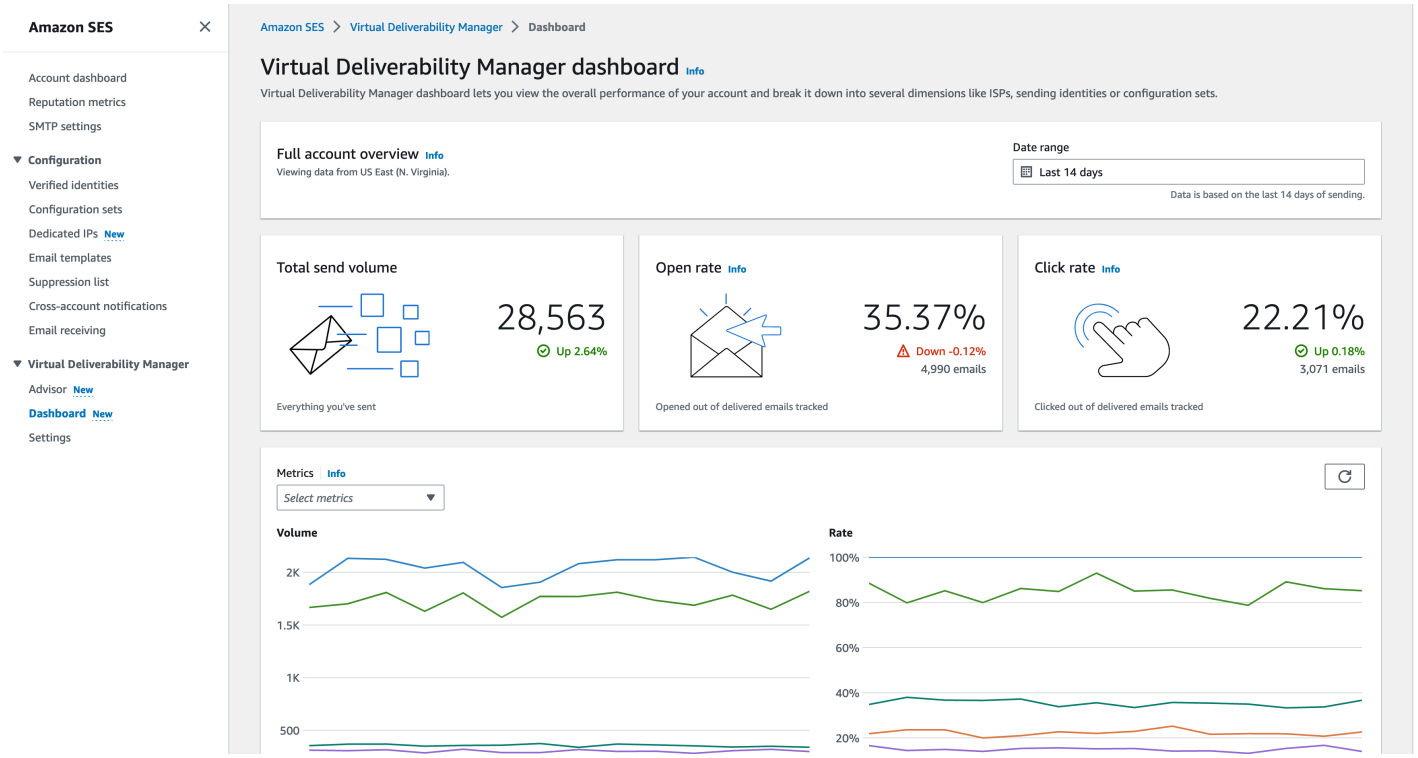
- Pour définir des paramètres personnalisés indiquant comment un jeu de configurations utilisera le suivi de l'engagement et la livraison partagée optimisée en remplaçant leur définition dans Virtual Deliverability Manager, consultez l'exemple de l'AWS CLIdans the section called “Paramètres”.

Tableau de bord Virtual Deliverability Manager

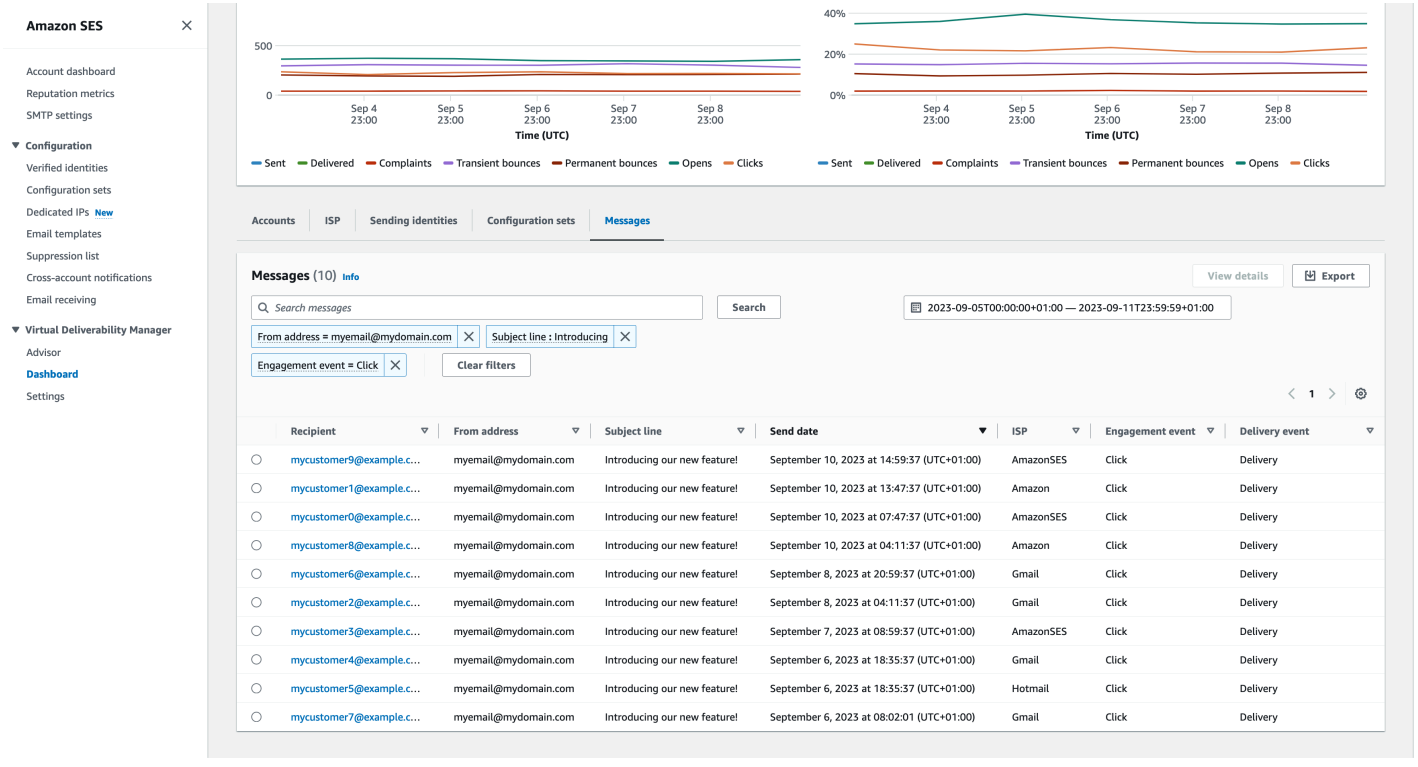
Le tableau de bord offre une vue globale du programme de délivrabilité de votre compte, avec par exemple des cartes et des graphiques chronologiques faciles à lire qui indiquent la délivrabilité et la réputation à travers les taux d'ouverture/de clics et de livraison, ainsi que les statistiques de retours à l'expéditeur/réclamations. Le tableau de bord offre également une vue plus détaillée, qui vous permet d'accéder à des données de tableau plus détaillées en cas de problème lié à un FAI, à une identité d'envoi ou à un jeu de configurations associé à une campagne par e-mail.

Le fait de pouvoir voir les choses à un niveau global tout en ayant la possibilité d'afficher des détails spécifiques vous permet de vous concentrer sur les aspects problématiques de votre délivrabilité plutôt que de devoir revoir votre programme de messagerie dans son ensemble. Ce niveau d'informations vous permet également de détecter les tendances et les soucis éventuels avant qu'ils ne se transforment en problèmes de délivrabilité plus importants, tels que des reports ou des blocages.

Vue d'ensemble d'un compte dans le tableau de bord Gestionnaire virtuel de diffusion présentant les cartes et les graphiques chronologiques.



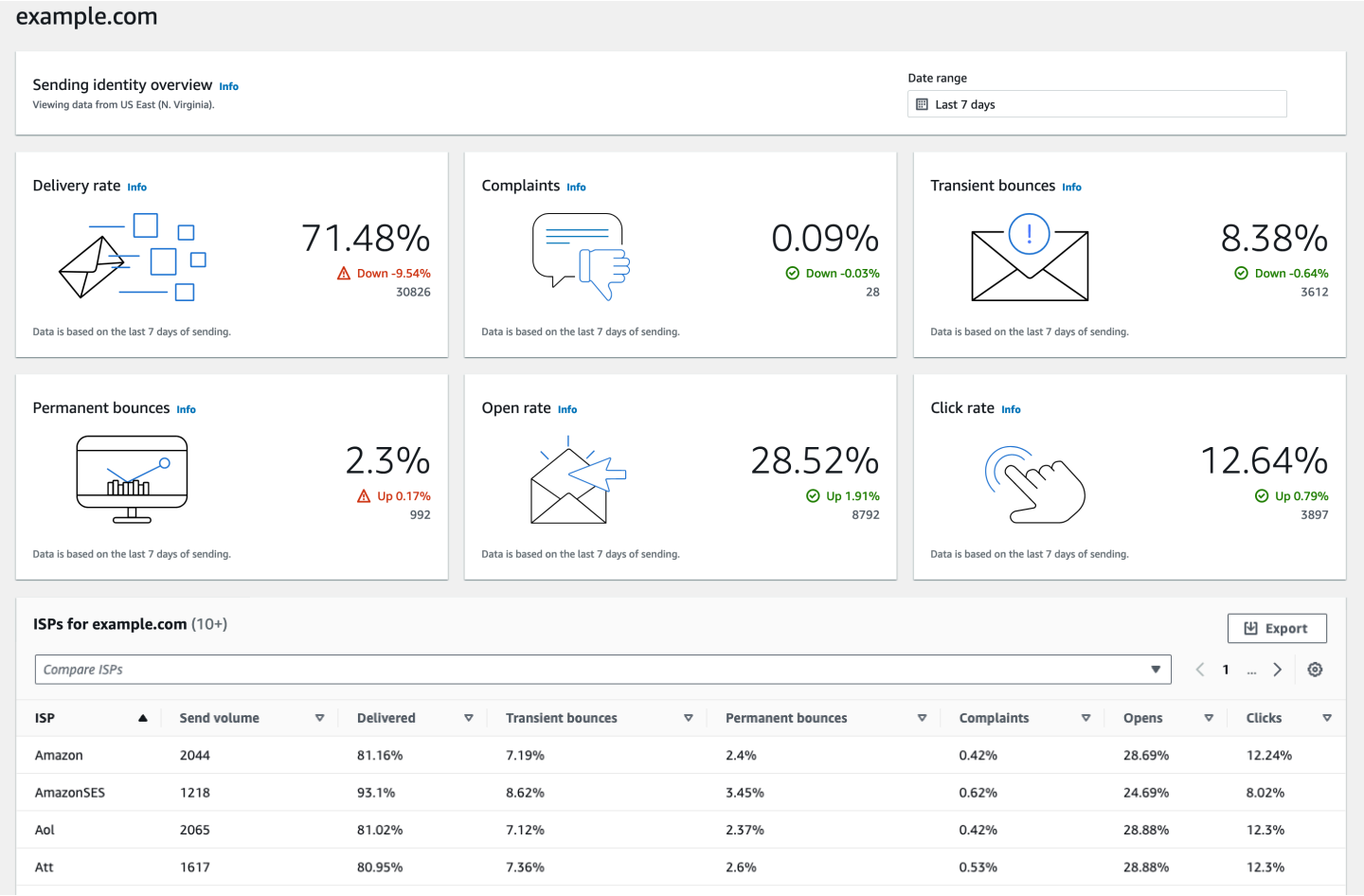
La table Messages sélectionnée dans le tableau de bord Gestionnaire virtuel de diffusion présentant les messages envoyés correspondant à la plage de dates et aux critères de filtrage.



Les données détaillées fournies par le tableau de bord peuvent vous aider à améliorer votre réputation d'expéditeur et à calculer les heures et les dates idéales afin d'améliorer l'engagement et les conversions pour votre programme de messagerie, avec la possibilité d'accéder à des jeux de données spécifiques :

- Données des FAI : précieuses lorsque vous rencontrez un problème de délivrabilité auprès d'un FAI ou d'un fournisseur de boîtes aux lettres en particulier. Au lieu d'essayer d'ajuster l'ensemble de votre compte, qui pourrait autrement fonctionner correctement, vous pouvez vous concentrer sur le point de terminaison problématique et vous conformer à ses bonnes pratiques afin d'améliorer la réputation de l'expéditeur envers ce FAI et de rétablir une bonne délivrabilité de la boîte de réception pour atteindre vos destinataires. Il est également important de comprendre la distribution de votre FAI, car vous pouvez effectuer plus d'envois à un FAI ou à un fournisseur de boîte aux lettres qu'à d'autres. Vous devez vous assurer que le trafic est toujours livré et engagé auprès des destinataires finaux pour avoir un impact positif sur la conversion de vos e-mails.
- Envoi de données d'identité et de jeux de configurations : utile pour vous aider à identifier les identités d'envoi et les jeux de configurations qui contribuent au problème global de délivrabilité de votre compte. Vous pouvez vous concentrer spécifiquement sur ces points, ajuster vos configurations et éventuellement réduire les envois à une identité particulière jusqu'à ce que le problème soit résolu. Par exemple, une identité d'envoi a été envoyée par erreur sur une liste de suppression, ce qui fait que tout le trafic passe par cette identité. Cette identité est associée à un jeu de configurations, ce qui entraîne des problèmes de délivrabilité. Dans de tels cas, il est utile de pouvoir identifier l'identité d'envoi ou du jeu de configurations afin de pouvoir vous concentrer sur la correction spécifique du problème, plutôt que de passer au peigne fin l'ensemble de votre compte pour essayer d'identifier la cause première du problème de délivrabilité.

Explorez en détails les données affichées dans le tableau de bord Gestionnaire virtuel de diffusion pour l'identité d'envoi sélectionnée, example.com : les cartes affichent des métriques de délivrabilité et de réputation. Le tableau affiche tous les FAI auxquels l'identité d'envoi a envoyé un e-mail avec des taux métriques pour chaque FAI dans la plage de dates saisie.



Utilisation du tableau de bord Virtual Deliverability Manager dans la console Amazon SES

La procédure suivante montre comment utiliser le tableau de bord Virtual Deliverability Manager dans la console Amazon SES pour consulter vos métriques globales de délivrabilité et de réputation et pour approfondir les domaines problématiques.

Pour utiliser le tableau de bord Virtual Deliverability Manager et afficher des données d'ensemble et plus détaillées des métriques de délivrabilité de votre compte

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le volet de navigation de gauche, choisissez Dashboard (Tableau de bord) sous Virtual Deliverability Manager.

> **Note**
>
> Dashboard (Tableau de bord) ne sera pas visible si vous n'avez pas activé Virtual Deliverability Manager pour votre compte. Pour plus d'informations, consultez the section called "Démarrer".

3. Dans le volet Présentation complète du compte, choisissez la plage de dates à utiliser pour toutes les métriques des cartes, des graphiques chronologiques et des tableaux déroulants.

   - Dans le champ Date range (Plage de dates), sélectionnez Relative range (Plage relative) (par défaut) ou Absolute range (Plage absolue).

     - Relative range (Plage relative) : sélectionnez la case d'option correspondant au nombre de jours souhaité.
       - Plage personnalisée : saisissez une plage en jours (jusqu'à 60), en semaines (jusqu'à 8) ou en mois (jusqu'à 2).
     - Plage absolue : la première date que vous choisissez est la Date de début et la deuxième est la Date de fin. Au total, la plage ne doit pas dépasser 60 jours. Pour spécifier un seul jour, choisissez-le à la fois comme Start date (Date de début) et End date (Date de fin).

   > **Note**
   >
   > Ce qui suit s'applique à toutes les plages de dates du tableau de bord :
   >
   > - Toutes les dates et heures sont exprimées en UTC.
   > - Pour les dates Relative range (Plage relative), le dernier jour se termine à minuit, heure UTC. Par exemple, si vous choisissez Last 7 days (7 derniers jours), le septième jour sera hier et se terminera à minuit.
   > - Si la plage de dates est supérieure à 30 jours, la colonne différence de % dans le tableau Statistiques de compte et les pourcentages de modification indiqués sur les cartes ne présentent pas de valeur (indiqué par un tiret -).

4. Les cartes, les graphiques chronologiques et tous les tableaux déroulants, Statistiques de compte, FSI, Identités d'envoi et Jeux de configurations, affichent les totaux des métriques calculés en fonction de la plage de dates saisie, et utilisent les formules de calcul de métriques décrites dans Comment les métriques du tableau de bord sont calculées.

- Pour créer un fichier `.csv` local contenant les données que vous consultez actuellement dans le tableau des fournisseurs d'accès à Internet, des identités d'envoi ou des jeux de configuration, sélectionnez le bouton Exporter.

5. Les graphiques chronologiques présentant la progression en Volume et Taux pour la plage de dates que vous avez saisie sont affichés dans le volet Métriques. Placez la souris sur un intervalle de dates dans les graphiques pour afficher le taux en pourcentage ou le volume exacts sur la base d'une agrégation journalière. Vous pouvez filtrer les métriques à afficher en utilisant la liste déroulante Sélectionner des métriques.
6. Cliquez sur l'onglet Accounts (Comptes) pour afficher le tableau Accounts statistics(Statistiques des comptes).

   - Ce tableau présente vos métriques de délivrabilité et de réputation, indiquant le Volume total, % Rate (Taux en %) et % Difference (Différence en %) pour Sent (E-mails envoyés), Delivered (E-mails livrés), Complaints (Réclamations), Transient & Permanent bounces (Retours à l'expéditeur transitoires et permanents) et Opens & Clicks (E-mails ouverts et clics), selon un calcul effectué à partir de la plage de dates saisie.

   > **Note**
   >
   > Si la plage de dates est supérieure à 30 jours, la colonne différence de % ne présente pas de valeur (indiqué par un tiret `-`).

7. Cliquez sur l'onglet ISP (FAI) pour afficher le tableau des ISP (FAI).

   - Ce tableau affiche les métriques relatives à Send volume (Volume d'envois), Delivered (E-mails livrés), Transient & Permanent bounces (Retours à l'expéditeur transitoires et permanents), Complaints (Réclamations) et Opens & Clicks (E-mails ouverts et clics) pour chaque FAI auquel vous avez envoyé des e-mails, selon un calcul effectué à partir de la plage de dates saisie.
   - Pour filtrer des FAI spécifiques, dans le champ de recherche Comparaison des ISP, cochez la case correspondant à chaque FAI à inclure.
   - Pour créer un fichier `.csv` local contenant les données que vous consultez actuellement dans ce tableau, sélectionnez le bouton Exporter.

8. Cliquez sur l'onglet Sending identities (Identités d'envoi) pour afficher le tableau Sending identities (Identités d'envoi).

- Ce tableau affiche les métriques relatives à Send volume (Volume d'envois), Delivered (E-mails livrés), Transient & Permanent bounces (Retours à l'expéditeur transitoires et permanents), Complaints (Réclamations) et Opens & Clicks (E-mails ouverts et clics) pour chaque identité d'envoi utilisée, selon un calcul effectué à partir de la plage de dates saisie.
- Pour filtrer des identités d'envoi spécifiques, dans le champ de recherche Comparer les identités, cochez la case correspondant à chaque identité à inclure.
- Pour explorer en détails une identité d'envoi spécifique, choisissez son nom dans la colonne Sending identity (Identité d'envoi).
  - Des cartes s'affichent avec les informations Taux de livraison, Réclamations, Retours à l'expéditeur transitoires et permanents et Taux d'e-mails ouverts et de clics pour l'identité d'envoi sélectionnée, selon un calcul effectué en fonction de la plage de dates saisie.
  - Les graphiques chronologiques sont actualisés et affichent toutes les métriques pour l'identité d'envoi sélectionnée, calculées en fonction de la plage de dates saisie.
  - Un tableau des FAI s'affichera, répertoriant tous les FAI auxquels l'identité d'envoi a envoyé des e-mails, avec des métriques données pour chaque FAI, selon un calcul effectué à partir de la plage de dates saisie.
- Pour créer un fichier `.csv` local contenant les données que vous consultez actuellement dans ce tableau, sélectionnez le bouton Exporter.

9. Cliquez sur l'onglet Configuration sets (Jeux de configurations) pour afficher le tableau Configuration sets (Jeux de configurations).

   - Ce tableau affiche les métriques relatives à Send volume (Volume d'envois), Delivered (E-mails livrés), Transient & Permanent bounces (Retours à l'expéditeur transitoires et permanents), Complaints (Réclamations) et Opens & Clicks (E-mails ouverts et clics) pour chaque jeu de configurations utilisé, selon un calcul effectué à partir de la plage de dates saisie.
   - Pour filtrer des jeux de configurations spécifiques, dans la zone de recherche Choisir des jeux de configurations, cochez la case correspondant à chaque jeu de configurations à inclure.
   - Pour filtrer un jeu de configurations spécifique, choisissez son nom dans la colonne Configuration set (Jeu de configurations).
     - Des cartes s'affichent avec les informations Taux de livraison, Réclamations, Retours à l'expéditeur transitoires et permanents et Taux d'e-mails ouverts et de clics pour le jeu de configurations sélectionné, selon un calcul effectué en fonction de la plage de dates saisie.

- Les graphiques chronologiques sont actualisés et affichent toutes les métriques pour le jeu de configuration sélectionné, calculées en fonction de la plage de dates saisie.
- Un tableau des FAI s'affichera, répertoriant tous les FAI pour lesquels le jeu de configurations a été utilisé afin d'envoyer des e-mails, avec des métriques données pour chaque FAI, selon un calcul effectué à partir de la plage de dates saisie.

- Pour créer un fichier `.csv` local contenant les données que vous consultez actuellement dans ce tableau, sélectionnez le bouton Exporter.

10. Choisissez l'onglet Messages pour afficher la table Messages.

    Il s'agit d'une table interactive qui vous permet de rechercher et de retrouver les messages que vous avez envoyés. Pour chaque message, vous pouvez suivre son état actuel de livraison et d'engagement, consulter l'historique des événements et voir la réponse renvoyée par le fournisseur de boîte aux lettres. Les points suivants décrivent les manières dont vous pouvez rechercher des messages spécifiques :

    - Vous pouvez effectuer une sélection dans le sélecteur de plage de dates, afin de filtrer les messages que vous avez envoyés au cours des 30 derniers jours. Si vous ne sélectionnez aucune plage de dates, votre recherche porte par défaut sur les 7 derniers jours, y compris le jour actuel dans votre fuseau horaire.
    - Dans le champ Rechercher des messages, vous pouvez filtrer sur Destinataire, Adresse d'expédition, Objet, FSI, Événement d'engagement, Événement de livraison et ID de message. Les propriétés suivantes s'appliquent :
        - Selon le type de filtre, vous pouvez saisir une chaîne de texte sensible à la casse ou sélectionner une valeur dans une liste.
        - Le paramètre Événement d'engagement est limité à une seule valeur, alors que le paramètre Objet peut avoir jusqu'à deux valeurs, et tous les autres filtres peuvent avoir jusqu'à cinq valeurs par recherche. Le filtrage par ID de message exclut tous les autres filtres que vous pourriez avoir sélectionnés, y compris la plage de dates.
        - La colonne ID de message est masquée par défaut, mais peut être affichée en sélectionnant l'icône en forme de roue dentée pour personnaliser la façon dont vous visualisez la table Messages.
    - Après avoir sélectionné vos filtres et une plage de dates, choisissez Rechercher pour remplir la table avec les messages correspondant à vos critères de recherche. La table peut charger jusqu'à 100 messages. Si votre recherche renvoie plus de 100 messages, les 100 messages présentés dans le tableau sont un échantillon aléatoire du total renvoyé.

- Le fait de cocher la case d'option d'un message et de sélectionner Afficher les détails affiche une barre latérale Informations sur le message contenant les détails de l'historique complet des événements du message, avec le plus récent en haut, et toutes les réponses ou tous les codes de diagnostic renvoyés par le fournisseur de boîte aux lettres.
- Pour créer un fichier `.csv` local contenant les données que vous consultez actuellement dans ce tableau, sélectionnez le bouton Exporter.

Accès à vos données de métriques Virtual Deliverability Manager à l'aide de l' AWS CLI

L'exemple suivant montre comment accéder à vos données de métriques Virtual Deliverability Manager à l'aide de l' AWS CLI. Il s'agit des mêmes données utilisées dans le tableau de bord Virtual Deliverability Manager dans la console.

Pour accéder à vos données métriques de délivrabilité à l'aide du AWS CLI

Vous pouvez utiliser l'opération `BatchGetMetricData` dans l'API Amazon SES v2 pour accéder à vos données de métriques de délivrabilité. Vous pouvez appeler cette opération depuis l' AWS CLI , comme illustré dans les exemples suivants.

- Accédez à vos données de métriques de délivrabilité :

```
aws --region us-east-1 sesv2 batch-get-metric-data --cli-input-json file://sends.json
```

- Le fichier d'entrée ressemble à ceci :

```
{
 "Queries": [
   {
     "Id": "Retrieve-Account-Sends",
     "Namespace": "VDM",
     "Metric": "SEND",
     "StartDate": "2022-11-04T00:00:00",
     "EndDate": "2022-11-05T00:00:00"
    }
 ]
}
```

Vous pouvez trouver plus d'informations sur les valeurs des paramètres et les types de données qui y sont associés à partir du type de données `BatchGetMetricDataQuery` figurant dans la référence de l'API Amazon SES v2.

Filtrer et exporter vos données métriques de délivrabilité à l'aide du AWS CLI

Cet exemple vous montre comment utiliser l'opération `CreateExportJob` pour filtrer et exporter vos données de métriques de délivrabilité vers un fichier .csv ou .json à l'aide de l'interface AWS CLI. Il s'agit des mêmes données que celles utilisées dans les tables FSI, Identités d'envoi et Jeu de configurations du tableau de bord du Gestionnaire virtuel de diffusion.

Pour filtrer et exporter vos données métriques de délivrabilité vers un fichier .csv ou .json à l'aide du AWS CLI

Vous pouvez utiliser l'opération `CreateExportJob` avec le type de données `MetricsDataSource` dans l'API v2 d'Amazon SES pour filtrer et exporter vos données de métriques vers un fichier .csv ou .json. Vous appelez cette opération à partir du AWS CLI , comme indiqué dans l'exemple suivant.

- Filtrez et exportez vos données de métriques de délivrabilité à l'aide d'un fichier d'entrée :

```
aws --region us-east-1 sesv2 create-export-job --cli-input-json file://metric-export-input.json
```

- Dans cet exemple, le fichier d'entrée utilise les paramètres `MetricsDataSource` pour filtrer les fournisseurs de services Internet auxquels vous avez envoyé du courrier, indiquant le taux de livraison réussie dans la plage de dates donnée, ainsi qu'un format .csv spécifié pour le fichier de sortie :

```
{
    "ExportDataSource": {
        "MetricsDataSource": {
            "Dimensions": {
                "ISP": ["*"]
            },
            "Namespace": "VDM",
            "Metrics": [
                {
```

```
                    "Name": "DELIVERY",
                    "Aggregation": "RATE"
                }
            ],
            "StartDate": "2023-06-13T00:00:00",
            "EndDate": "2023-06-20T00:00:00"
        }
    },
    "ExportDestination": {
        "DataFormat": "CSV"
    }
}
```

Vous pouvez trouver plus d'informations sur les valeurs des paramètres et les types de données qui y sont associés dans `MetricsDataSource`, objet de type `ExportDataSource` dans la référence de l'API v2 d'Amazon SES.

Trouver les messages que vous avez envoyés, leur statut de livraison et d'engagement, et exporter les résultats à l'aide du AWS CLI

Ces exemples montrent comment utiliser l'opération `CreateExportJob` pour rechercher et trouver des messages spécifiques que vous avez envoyés, consulter leur statut actuel de livraison et d'engagement, et exporter les résultats de votre recherche dans un fichier .csv ou .json à l'aide de l'interface AWS CLI. Il s'agit des mêmes données que celles utilisées dans la table Messages du tableau de bord du Gestionnaire virtuel de diffusion.

Pour rechercher les messages envoyés, leur état de livraison et d'engagement, et exporter les résultats vers un fichier .csv ou .json à l'aide du AWS CLI

Vous pouvez utiliser l'opération `CreateExportJob` avec le type de données `MessageInsightsDataSource` dans l'API v2 d'Amazon SES pour appliquer des filtres afin de trouver des messages spécifiques que vous avez envoyés, de consulter leur statut de livraison et d'engagement, et d'exporter les résultats dans un fichier .csv ou .json. Vous appelez cette opération à partir du AWS CLI , comme indiqué dans les exemples suivants.

> **Note**
>
> Si votre recherche filtrée renvoie plus de 10 000 messages, les 10 000 messages figurant dans l'ensemble de résultats de l'API sont un échantillon aléatoire du total renvoyé.

- Recherchez des messages envoyés, consultez leur statut actuel et exportez les résultats à l'aide d'un fichier d'entrée :

```
aws --region us-east-1 sesv2 create-export-job --cli-input-json file://message-insights-export-input.json
```

- Dans cet exemple, le fichier d'entrée utilise les paramètres `MessageInsightsDataSource` pour filtrer un sujet intitulé « Sale Ends Tonight! » (La vente se termine ce soir !) et un format .csv spécifié pour le fichier de sortie :

```
{
    "ExportDataSource": {
        "MessageInsightsDataSource": {
            "StartDate": "2023-07-01T00:00:00",
            "EndDate": "2023-07-10T00:00:00",
            "Include": {
                "Subject": [
                    "Sale Ends Tonight!"
                ]
            }
        }
    },
    "ExportDestination": {
        "DataFormat": "CSV"
    }
}
```

- Dans cet exemple, le fichier d'entrée utilise des `MessageInsightsDataSource`paramètres pour filtrer un sujet commençant par « Hello », envoyé avec une « information » FromEmailAddress contenant des « informations » vers des destinations se terminant par « @example .com », et un format .json spécifié pour le fichier de sortie :

```
{
    "ExportDataSource": {
        "MessageInsightsDataSource": {
            "StartDate": "2023-07-01T00:00:00",
            "EndDate": "2023-07-10T00:00:00",
            "Include": {
                "Subject": [
                    "Hello*"
```

```
                ],
                "FromEmailAddress": [
                    "*information*"
                ],
                "Destination": [
                    "*@example.com"
                ]
            }
        }
    },
    "ExportDestination": {
        "DataFormat": "JSON"
    }
}
```

- Dans cet exemple, le fichier d'entrée utilise des `MessageInsightsDataSource`paramètres pour filtrer un sujet commençant par « Bonjour », exclure les résultats contenant « noreply@example.com » en tant que tel et un FromEmailAddress format .csv spécifié pour le fichier de sortie :

```
{
    "ExportDataSource": {
        "MessageInsightsDataSource": {
            "StartDate": "2023-07-01T00:00:00",
            "EndDate": "2023-07-10T00:00:00",
            "Include": {
                "Subject": [
                    "Hello*"
                ]
            },
            "Exclude": {
                "FromEmailAddress": [
                    "noreply@example.com"
                ]
            }
        }
    },
    "ExportDestination": {
        "DataFormat": "CSV"
    }
}
```

- Dans cet exemple, le fichier d'entrée utilise des `MessageInsightsDataSource`paramètres pour filtrer un sujet commençant par « Bonjour », envoyé avec une « information » FromEmailAddress contenant des « informations » vers des destinations se terminant par « @example .com », en utilisant Gmail comme fournisseur de services Internet, un dernier événement de livraison de « DELIVERY », un dernier événement d'engagement « OPEN » ou « CLICK », et un format .json spécifié pour le fichier de sortie :

```
{
    "ExportDataSource": {
        "MessageInsightsDataSource": {
            "StartDate": "2023-07-01T00:00:00",
            "EndDate": "2023-07-10T00:00:00",
            "Include": {
                "Subject": [
                    "Hello*"
                ],
                "FromEmailAddress": [
                    "*information*"
                ],
                "Destination": [
                    "*@example.com"
                ],
                "Isp": [
                    "Gmail"
                ],
                "LastDeliveryEvent": [
                    "DELIVERY"
                ],
                "LastEngagementEvent": [
                    "OPEN", "CLICK"
                ]
            }
        }
    },
    "ExportDestination": {
        "DataFormat": "JSON"
    }
}
```

- Dans cet exemple, le fichier d'entrée utilise des `MessageInsightsDataSource`paramètres pour filtrer les destinations se terminant par « @example1 .com », « @example2 .com » ou

« @example3 .com », pour exclure les messages dont le score est LastDeliveryEvent égal à « ENVOYER » ou « LIVRAISON » et au format .csv spécifié pour le fichier de sortie :

```
{
    "ExportDataSource": {
        "MessageInsightsDataSource": {
            "StartDate": "2023-07-01T00:00:00",
            "EndDate": "2023-07-10T00:00:00",
            "Include": {
                "Destination": [
                    "*@example1.com",
                    "*@example2.com",
                    "*@example3.com"
                ]
            },
            "Exclude": {
                "LastDeliveryEvent": [
                    "SEND",
                    "DELIVERY"
                ]
            }
        }
    },
    "ExportDestination": {
        "DataFormat": "CSV"
    }
}
```

Vous pouvez trouver plus d'informations sur les valeurs des paramètres et les types de données qui y sont associés dans `MessageInsightsDataSource`, objet de type `ExportDataSource` dans la référence de l'API v2 d'Amazon SES.

Gestion de vos tâches d'exportation à l'aide de l'interface AWS CLI

Ces exemples montrent comment gérer vos tâches d'exportation en les répertoriant, en obtenant des informations les concernant et en les annulant à l'aide de l'interface AWS CLI.

Pour répertorier vos tâches d'exportation à l'aide du AWS CLI

Vous pouvez utiliser l'opération `ListExportJobs` dans l'API v2 d'Amazon SES pour répertorier vos tâches d'exportation. Vous pouvez appeler cette opération à partir du AWS CLI , comme indiqué dans les exemples suivants.

- Répertoriez vos tâches d'exportation :

```
aws --region us-east-1 sesv2 list-export-jobs --export-source-type=METRICS_DATA
```

```
aws --region us-east-1 sesv2 list-export-jobs --job-status=CREATED
```

```
aws --region us-east-1 sesv2 list-export-jobs --cli-input-json file://list-export-jobs-input.json
```

- Le fichier d'entrée ressemble à ceci :

```
{
  "NextToken": "",
  "PageSize": 0,
  "ExportSourceType": "METRICS_DATA",
  "JobStatus": "CREATED"
}
```

  Plus d'informations sur les valeurs des paramètres pour l'opération `ListExportJobs` sont disponibles dans la référence de l'API v2 d'Amazon SES.

Pour obtenir des informations sur votre tâche d'exportation à l'aide du AWS CLI

Vous pouvez utiliser l'opération `GetExportJob` dans l'API v2 d'Amazon SES pour obtenir des informations sur votre tâche d'exportation. Vous pouvez appeler cette opération à partir du AWS CLI , comme indiqué dans les exemples suivants.

- Obtenez des informations sur votre tâche d'exportation :

```
aws --region us-east-1 sesv2 get-export-job --job-id=<JobId>
```

```
aws --region us-east-1 sesv2 get-export-job --cli-input-json file://get-export-job-input.json
```

- Le fichier d'entrée ressemble à ceci :

```
{
    "JobId": "e2220d6b-dce5-45f2-bf60-3287a465b732"
}
```

Plus d'informations sur les valeurs des paramètres pour l'opération `GetExportJob` sont disponibles dans la référence de l'API v2 d'Amazon SES.

Pour annuler votre tâche d'exportation à l'aide du AWS CLI

Vous pouvez utiliser l'opération `CancelExportJob` dans l'API v2 d'Amazon SES pour annuler votre tâche d'exportation. Vous pouvez appeler cette opération à partir du AWS CLI , comme indiqué dans les exemples suivants.

- Annulez votre tâche d'exportation :

```
aws --region us-east-1 sesv2 cancel-export-job --job-id=<JobId>
```

```
aws --region us-east-1 sesv2 cancel-export-job --cli-input-json file://cancel-export-job-input.json
```

- Le fichier d'entrée ressemble à ceci :

```
{
    "JobId": "e2220d6b-dce5-45f2-bf60-3287a465b732"
}
```

Plus d'informations sur les valeurs des paramètres pour l'opération `CancelExportJob` sont disponibles dans la référence de l'API v2 d'Amazon SES.

Consulter l'historique complet des événements d'un message et les réponses des fournisseurs de services Internet à l'aide du AWS CLI

L'exemple suivant montre comment consulter les détails de l'historique complet des événements d'un message ainsi que les réponses ou les codes de diagnostic renvoyés par le fournisseur de boîte aux lettres à l'aide de l'interface AWS CLI. Il s'agit des mêmes données que celles utilisées dans la barre

latérale Informations sur le message après la sélection de la case d'option d'un message dans la table Messages du tableau de bord du Gestionnaire virtuel de diffusion.

Pour consulter l'historique des événements d'un message et les réponses du fournisseur de services Internet à l'aide du AWS CLI

Vous pouvez utiliser l'opération `GetMessageInsights` dans l'API v2 d'Amazon SES pour voir les détails d'un message envoyé. Vous pouvez appeler cette opération à partir du AWS CLI , comme indiqué dans l'exemple suivant.

- Consultez les détails concernant un e-mail envoyé, identifié par son ID de message :

```
aws --region us-east-1 sesv2 get-message-insights --message-id
 01000100001000dd-2a19190d-99d4-0000-9f00-deb5bbf2bfbe-000001
```

  Plus d'informations sur les valeurs des paramètres pour l'opération `GetMessageInsights` sont disponibles dans la référence de l'API v2 d'Amazon SES.

Comment les métriques du tableau de bord Virtual Deliverability Manager sont calculées

Toutes les cartes de taux et les tableaux déroulants affichés dans le tableau de bord Gestionnaire virtuel de diffusion calculent les métriques relatives à la plage de dates saisie dans le volet Présentation complète du compte.

Les pourcentages des taux de métriques affichés dans le tableau de bord sont calculés comme décrit dans le tableau. Les quatre dernières colonnes représentent les qualificatifs des mathématiques de base utilisées pour calculer les métriques affichées. Par exemple, votre Open rate (Taux d'ouverture) est calculé comme le nombre total d'ouvertures divisé par le total des messages HTML envoyés avec le suivi de l'engagement activé. Il ne reflète aucun des messages envoyés sans suivi de l'engagement et qui ne sont pas encodés en HTML.

Rate % (% du taux)	Comment le calculer	Avec le suivi des engagements activé et HTML	Et avec au moins 1 lien suivi	Livré aux FAI dotés d'une FBL (Boucle de rétroaction) SES	Exclu s'il fait partie de votre liste de suppression au niveau du compte
Open rate (Taux d'ouverture)	total ouvert/total livré	✗			
Click rate (Taux de clics)	total de clics/total livré	✗	✗		
Complaint rate (Taux de réclamations)	total de réclamations/total livré			✗	✗
Delivery rate (Taux de remise)	total livré/total envoyé				
Transient bounce rate (Taux de retours à l'expéditeur transitoires)	total de retours à l'expéditeur transitoires/total envoyé				✗
Permanent bounce rate (Taux de retours à l'expéditeur permanents)	total de retours à l'expéditeur permanents/total envoyé				✗
Total send volume (Volume envoyé total)	% du taux non affiché (tout ce que vous avez envoyé ; toujours 100 %)				

Comment le taux de différence et les volumes totaux sont calculés pour toutes les métriques :

- Difference % (% de différence) : différence entre le total de métriques et le total de métriques précédent pour la plage de dates donnée. Par exemple, si Last 7 days (7 derniers jours) est la plage de dates spécifiée, Metric rate of last 7 days - Metric rate of previous 7 days (Taux de métriques des 7 derniers jours - Taux de métriques des 7 jours précédents).
  - Le % de différence pour Total send volume (Volume envoyé total) est calculé différemment. Par exemple, (Send volume of last 7 days - Send volume of previous 7 days) / Send volume of previous 7 days ((Volume d'envoi des 7 derniers jours - Volume d'envoi des 7 jours précédents)/ Volume d'envoi des 7 derniers jours)).
- Volume : nombre total de chaque métrique.

> **Note**
>
> - La colonne Delivered (Livré) des tableaux déroulants affiche le volume livré directement, sans les qualificatifs de livraison utilisés pour calculer les taux d'ouverture, de clics et de réclamations.
> - Virtual Deliverability Manager ne suit que les métriques des e-mails ayant un seul destinataire. Les e-mails ayant plusieurs destinataires ne sont pris en compte dans aucune des métriques du tableau de bord Virtual Deliverability Manager.
>   - Dans ces cas, le nombre de métriques de votre Virtual Deliverability Manager sera inférieur à celui d'Amazon CloudWatch , car CloudWatch les statistiques incluent les e-mails avec plusieurs destinataires.
> - Les e-mails envoyés à SES mailbox simulator (Simulateur de boîtes aux lettres SES) ne sont pris en compte dans aucune des métriques du tableau de bord Virtual Deliverability Manager.
> - Les e-mails envoyés via le compte d'un expéditeur délégué (auparavant appelé « envoi inter-comptes ») ne sont pris en compte dans aucune des métriques du tableau de bord du Gestionnaire virtuel de diffusion.

> **Important**
>
> La protection de la vie privée d'Apple Mail et son impact sur les taux d'engagement : suite à la mise en œuvre par Apple de sa fonction de protection de la confidentialité dans Mail

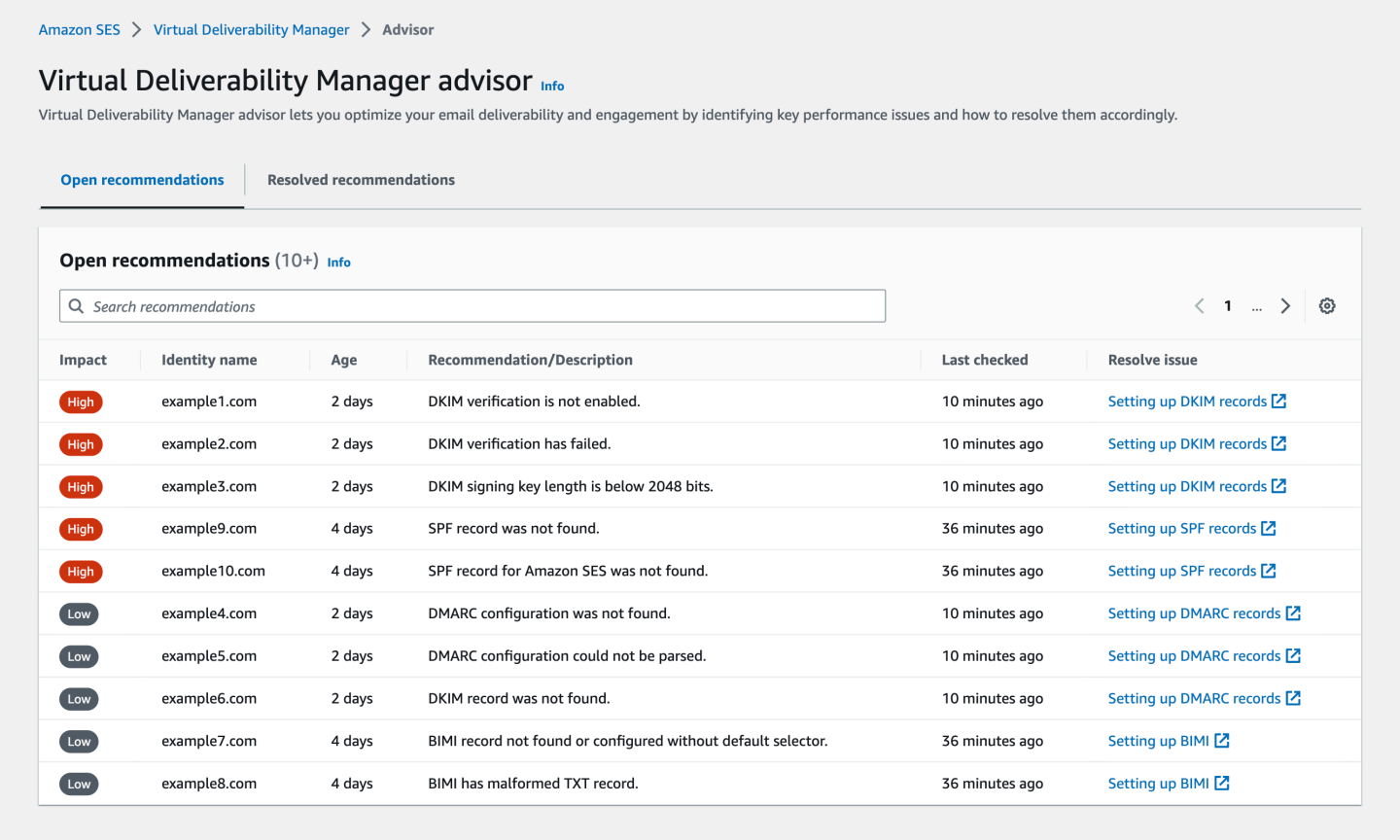
(MPP) pour les appareils Apple à partir d'iOS 15, les chiffres d'engagement ont augmenté. En effet, les déclencheurs MPP s'ouvrent lorsque l'application Apple Mail est lancée, pas nécessairement lorsqu'un destinataire ouvre et/ou clique sur un message. Les données d'engagement semblent donc beaucoup plus élevées qu'elles ne le seraient normalement et c'est un élément que les professionnels du marketing par e-mail devront prendre en compte lors de l'évaluation de l'engagement. Il existe plusieurs autres moyens d'identifier l'engagement, tels que l'activité sur le web, l'utilisation des applications/portails et l'utilisation de données proxy provenant d'appareils autres qu'Apple pour créer une métrique agrégée. Il est important de se concentrer sur les tendances en matière d'engagement, car elles peuvent indiquer s'il y a un problème avec l'envoi de vos e-mails. Pour plus d'informations sur la protection de la confidentialité, consultez Apple Mail's Privacy Protection (Protection de la confidentialité dans Mail d'Apple).

Conseiller Virtual Deliverability Manager

Le conseiller Virtual Deliverability Manager vous aide à optimiser la délivrabilité et l'engagement de vos e-mails en identifiant les principaux problèmes de performance et d'infrastructure du compte et les niveaux d'identité d'envoi qui nuisent à la délivrabilité et à la réputation de vos e-mails. Il offre des solutions en fournissant des conseils spécifiques sur la manière de résoudre le problème identifié.

Les recommandations d'infrastructure du conseiller sont répertoriées dans le tableau Open recommendations (Recommandations en cours). Vous y trouverez les problèmes d'authentification de courrier électronique classiques, tels que des enregistrements SPF, DKIM, DMARC ou BIMI inexistants ou présentant des problèmes de configuration, notamment s'ils sont malformés ou que leur clé est trop courte. Elles sont classées par gravité de l'Impact, par Identity name (Nom d'identité) du domaine expéditeur et par Age (Âge) de l'alerte. Dans la barre de recherche, une zone de liste permet de filtrer par niveau d'impact, catégorie d'infrastructure ou nom de l'identité d'envoi. La colonne Last checked (Dernière vérification) indique l'heure relative de la dernière mise à jour de la recommandation, par exemple « à l'instant » ou « il y a 15 minutes ». La dernière colonne, Resolve issue (Résoudre le problème), contient un lien vers la section correspondante du Guide du développeur Amazon SES offrant des conseils sur la manière de résoudre le problème identifié.

Les recommandations ouvertes s'affichent dans le conseiller Virtual Deliverability Manager, triées par niveau d'impact.



Si vous n'avez aucune notification en cours de votre conseiller, un message indiquera qu'aucune recommandation n'est ouverte. Nous vous recommandons de consulter régulièrement le conseiller. Vous pouvez éventuellement intégrer ces événements de notification destinés aux conseillers EventBridge à Amazon pour créer des applications évolutives axées sur les événements, comme expliqué dans. Surveillance à l'aide EventBridge

Vous pouvez également accéder au tableau Resolved recommendations (Recommandations résolues) depuis la page du conseiller Virtual Deliverability Manager, qui répertorie les problèmes d'infrastructure que vous avez résolus en mettant en œuvre les conseils du conseiller. Les recommandations résolues sont répertoriées avec un statut initial qui décrit le problème avant qu'il ne soit résolu. Les recommandations résolues expirent au bout de 30 jours.

Ce que recherche le conseiller du Virtual Deliverability Manager

Dans la section précédente, nous avons expliqué que le conseiller de Virtual Deliverability Manager effectue des vérifications par rapport à votre domaine d'envoi afin de déterminer si vous avez configuré une infrastructure authentifiée en toute sécurité afin de vous assurer de maintenir un taux élevé de délivrabilité des e-mails et de conserver une bonne réputation d'expéditeur. Avant

d'activer le conseiller Virtual Deliverability Manager, nous pensons qu'il serait utile que vous sachiez exactement ce que le conseiller vérifie et ce qu'il recherche dans ces vérifications.

Vous pouvez utiliser ce tableau comme référence pour passer en revue la configuration de votre domaine d'envoi et corriger les éléments qui ne sont pas conformes aux normes répertoriées dans ce tableau avant qu'ils ne deviennent des problèmes que le conseiller doit vous signaler.

Type de chèque	Message du conseiller	Pourquoi le conseiller vous alerte	En savoir plus
Configuration DKIM	La vérification DKIM n'est pas activée.	Le DKIM n'est pas activé par identité.	Easy DKIM dans SES
Principal atout du DKIM	La longueur de la clé de signature DKIM est inférieure à 2048 bits.	La longueur de la clé de signature DKIM n'utilise pas au moins 2 048 bits.	Easy DKIM dans SES
Validation des enregistrements DNS DKIM	La vérification DKIM a échoué.	Les enregistrements DKIM CNAME ont été jugés non valides après avoir recherché et essayé de valider la clé.	Vérification de l'identité d'un domaine DKIM auprès de votre fournisseur DNS
Configuration du DMARC	La configuration DMARC est introuvable.	Les enregistrements DMARC TXT sont manquants.	Configuration de la politique DMARC sur votre domaine
Vérification du format d'enregistrement DNS DMARC	La configuration DMARC n'a pas pu être analysée.	Format non valide détecté pour les enregistrements DMARC TXT.	Configuration de la politique DMARC sur votre domaine
Configuration DKIM du DMARC	Aucun enregistrement DKIM n'a été trouvé.	Aucun enregistrement DKIM n'a été trouvé afin de se conformer au DMARC.	Conformité au DMARC via DKIM

Type de chèque	Message du conseiller	Pourquoi le conseiller vous alerte	En savoir plus
Configuration DKIM du DMARC	L'enregistrement DKIM n'est pas aligné.	Le domaine spécifié dans la signature DKIM ne correspon d pas au domaine indiqué dans l'adresse d'origine.	Conformité au DMARC via DKIM
Configuration du SPF	Aucun enregistrement SPF n'a été trouvé.	Enregistrement TXT SPF manquant pour le domaine MAIL FROM personnalisé.	Configuration de votre domaine MAIL FROM personnalisé
SPF « inclus » configuré	L'enregistrement SPF pour Amazon SES est introuvable.	`include:amazonses.com` est absent de l'enregis trement TXT SPF.	Configuration de votre domaine MAIL FROM personnalisé
Application du SPF configurée	Il manque le qualifica tif SPF all.	`~all`est absent de l'enregistrement TXT SPF.	Configuration de votre domaine MAIL FROM personnalisé
Validation de l'applica tion du SPF	Un problème de configuration SPF a été détecté.	Les tentatives de détection de l'enregis trement SPF MX requis dans les 72 heures ont échoué.	États de configura tion du domaine MAIL FROM personnalisé
BIMI configuré	Enregistrement BIMI introuvable ou configuré sans sélecteur par défaut.	Les enregistrements BIMI TXT sont absents ou ne possèdent pas l'attribut de sélection.	Configuration du BIMI

Type de chèque	Message du conseiller	Pourquoi le conseiller vous alerte	En savoir plus
Validation du format BIMI	BIMI a un enregistrement TXT mal formé.	L'enregistrement BIMI TXT a été déterminé comme étant mal configuré après vérification de la présence et du format valide des éléments suivants : version, URL du certificat et URL du logo.	Configuration du BIMI

Utilisation du conseiller Virtual Deliverability Manager dans la console Amazon SES

La procédure suivante vous montre comment utiliser le conseiller Virtual Deliverability Manager dans la console Amazon SES pour résoudre les problèmes de délivrabilité identifiés à l'aide de la console Amazon SES.

Pour utiliser le conseiller Virtual Deliverability Manager afin de résoudre des problèmes de délivrabilité et de réputation

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le volet de navigation de gauche, choisissez Advisor (Conseiller) sous Virtual Deliverability Manager.

> **Note**
>
> Advisor (Conseiller) ne sera pas visible si vous n'avez pas activé Virtual Deliverability Manager pour votre compte. Pour plus d’informations, consultez the section called “Démarrer”.

3. Open recommendations table (Tableau des recommandations ouvertes) s'affiche par défaut. Les recommandations sont classées par Impact (élevé/faible), Identity name (Nom d'identité) (domaine d'envoi), Age (Âge) (de l'alerte) et Recommendation/Description (Recommandation/description) (problème identifié). Dans la barre de recherche, filtrez en fonction du niveau d'Impact, de la Category (Catégorie) du problème d'infrastructure ou du Identity name (Nom d'identité) du domaine d'envoi.
4. Pour résoudre un problème décrit dans la colonne Recommendation/Description (Recommandation/description), cliquez sur le lien dans la colonne Resolve issue (Résoudre le problème) correspondant à cette ligne et mettez en œuvre la solution suggérée.

> **Note**
>
> Une fois que vous avez mis en œuvre une solution, le problème résolu peut prendre jusqu'à six heures pour être reflété. Vous pouvez afficher le problème résolu dans l'onglet Resolved recommendations (Recommandations résolues).

Accès à vos recommandations Virtual Deliverability Manager à l'aide de l' AWS CLI

Les exemples suivants montrent comment accéder aux recommandations Virtual Deliverability Manager à l'aide de l' AWS CLI.

Pour accéder aux recommandations de votre Virtual Deliverability Manager à l'aide du AWS CLI

Vous pouvez utiliser l'opération `ListRecommendations` dans l'API Amazon SES v2 pour répertorier vos recommandations de délivrabilité. Vous pouvez appeler cette opération depuis l' AWS CLI, comme illustré dans les exemples suivants.

- Répertoriez les recommandations pour voir les problèmes de délivrabilité :

```
aws --region us-east-1 sesv2 list-recommendations
```

- Appliquez des filtres pour récupérer les recommandations relatives à un domaine spécifique que vous possédez :

```
aws --region us-east-1 sesv2 list-recommendations --cli-input-json file://list-recommendations.json
```

- Le fichier d'entrée ressemble à ceci :

```
{
  "PageSize":100,
  "Filter":{
    "RESOURCE_ARN": "arn:aws:ses:us-east-1:123456789012:identity/example.com"
   }
}
```

Paramètres de Virtual Deliverability Manager

Vous pouvez consulter ou modifier les paramètres de Virtual Deliverability Manager sur votre compte à tout moment. Vous pouvez activer ou désactiver Virtual Deliverability Manager et spécifier un mode d'activation ou de désactivation pour le suivi de l'engagement et la livraison partagée optimisée au niveau du compte Virtual Deliverability Manager via la console Amazon SES ou l'AWS CLI.

Les options de Virtual Deliverability Manager sont également fournies au niveau du jeu de configurations afin que vous puissiez définir des paramètres personnalisés indiquant comment un jeu de configurations utilisera le suivi de l'engagement et la livraison partagée optimisée en remplaçant leur définition dans Virtual Deliverability Manager. Cela vous donne la possibilité d'adapter l'envoi de vos e-mails pour des campagnes d'e-mails spécifiques. Par exemple, vous pouvez activer le suivi de l'engagement et la livraison partagée optimisée pour vos e-mails marketing et les désactiver pour vos e-mails transactionnels.

Modification vos paramètres de compte Virtual Deliverability Manager à l'aide de la console Amazon SES

La procédure suivante décrit comment modifier vos paramètres de compte Virtual Deliverability Manager à l'aide de la console Amazon SES.

Pour modifier vos paramètres de compte Virtual Deliverability Manager à l'aide de la console Amazon SES

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES sur la page https://console.aws.amazon.com/ses/.
2. Dans le volet de navigation de gauche, choisissez Settings (Paramètres) sous Virtual Deliverability Manager.

La page Virtual Deliverability Manager settings (Paramètres de Virtual Deliverability Manager) s'ouvre. Le volet Subscription overview (Présentation des abonnements) indique le statut de Virtual Deliverability Manager et le volet Additional settings (Paramètres supplémentaires) indique le statut de Engagement tracking (Suivi de l'engagement) et de Optimized shared delivery (Livraison partagée optimisée).

3. Pour modifier les paramètres Engagement tracking (Suivi de l'engagement) ou Optimized shared delivery (Livraison partagée optimisée) :

   a. Dans le volet Additional settings (Paramètres supplémentaires), choisissez Edit (Modifier).

   b. Sélectionnez la case d'option correspondante pour activer ou désactiver l'une des fonctionnalités, puis choisissez Submit settings (Soumettre les paramètres).

      La page Virtual Deliverability Manager settings (Paramètres de Virtual Deliverability Manager) affiche un résumé de vos modifications dans le volet Additional settings (Paramètres supplémentaires).

      > **Note**
      >
      > Les options Engagement tracking (Suivi de l'engagement) que vous définissez ici ou dans les paramètres de configuration de Virtual Deliverability Manager, contrôlent si les ouvertures et les clics doivent être signalés ou non dans le tableau de bord de Virtual Deliverability Manager ; elles n'affectent pas les configurations de destination des événements qui publient les événements d'ouverture et de clic. Par exemple, si vous avez désactivé le suivi de l'engagement ici, cela ne désactivera pas la publication des événements d'ouverture et de clic que vous avez configurés dans les destinations d'événements SES.

4. (Facultatif) Pour définir des paramètres personnalisés concernant la manière dont un jeu de configurations utilise le suivi de l'engagement et la livraison partagée optimisée en remplaçant leur définition dans Virtual Deliverability Manager, consultez Virtual Deliverability Manager options (Options de Virtual Deliverability Manager) lors de la création ou de la modification d'un jeu de configurations.

5. Pour désactiver Virtual Deliverability Manager :

   a. Dans le volet Subscription overview (Présentation des abonnements), choisissez Disable Virtual Deliverability Manager (Désactiver Virtual Deliverability Manager).

b. Dans la fenêtre contextuelle Disable Virtual Deliverability Manager? (Désactiver Virtual Deliverability Manager ?), saisissez *Disable* dans le champ de confirmation, puis choisissez Disable Virtual Deliverability Manager (Désactiver Virtual Deliverability Manager).

c. Une bannière s'affiche pour confirmer que vous avez désactivé Virtual Deliverability Manager.

6. Pour réactiver Virtual Deliverability Manager, consultez the section called “Démarrer”.

Modification de vos paramètres de compte Virtual Deliverability Manager à l'aide de la AWS CLI

Vous pouvez modifier vos paramètres de compte Virtual Deliverability Manager à l'aide de la AWS CLI.

Pour modifier vos paramètres de compte Virtual Deliverability Manager à l'aide de la AWS CLI

Vous pouvez utiliser les opérations `PutAccountVdmAttributes` et `PutConfigurationSetVdmOptions` de l'API Amazon SES v2 pour modifier vos paramètres Virtual Deliverability Manager. Vous pouvez appeler cette opération depuis l'AWS CLI, comme illustré dans les exemples suivants.

- Activez ou désactivez le suivi de l'engagement, la livraison partagée optimisée, ou les deux à l'aide d'un fichier d'entrée :

```
aws --region us-east-1 sesv2 put-account-vdm-attributes --cli-input-json file://
attributes.json
```

Dans cet exemple, où le suivi de l'engagement est `ENABLED` et la livraison partagée optimisée est `DISABLED`, le fichier d'entrée ressemble à ceci :

```
{
    "VdmAttributes": {
        "VdmEnabled": "ENABLED",
        "DashboardAttributes": {
            "EngagementMetrics": "ENABLED"
        },
        "GuardianAttributes": {
            "OptimizedSharedDelivery": "DISABLED"
        }
```

```
    }
}
```

Vous pouvez trouver plus d'informations sur les valeurs des paramètres et les types de données qui y sont associés en établissant un lien à partir du type de données `VdmAttributes` figurant dans la référence de l'API Amazon SES v2.

- Définissez des paramètres personnalisés indiquant comment un jeu de configurations utilisera le suivi de l'engagement et la livraison partagée optimisée en remplaçant leur définition dans Virtual Deliverability Manager :

```
aws --region us-east-1 sesv2 put-configuration-set-vdm-options --cli-input-json
 file://config-set.json
```

Dans cet exemple, où le suivi de l'engagement et la livraison partagée optimisée sont activés pour un jeu de configurations nommé example, le fichier d'entrée ressemble à ceci :

```
{
    "ConfigurationSetName": "example",
    "VdmOptions": {
        "DashboardOptions": {
            "EngagementMetrics": "ENABLED"
        },
        "GuardianOptions": {
            "OptimizedSharedDelivery": "ENABLED"
        }
    }
}
```

Pour plus d'informations sur les valeurs des paramètres et les types de données qui y sont associés, consultez le type de données `VdmOptions` dans la référence de l'API Amazon SES v2.

- Pour vérifier le résultat :

```
aws –region us-east-1 sesv2 get-configuration-set –configuration-set-name example
```

- Si vous ne spécifiez d'options `DashboardOptions` ou `GuardianOptions` au niveau du jeu de configurations, vos paramètres de compte Virtual Deliverability Manager s'appliquent au trafic envoyé via ce jeu de configurations.

Gestionnaire de messagerie pour Amazon SES

Mail Manager est un ensemble de fonctionnalités de passerelle de messagerie Amazon SES conçues pour vous aider à renforcer l'infrastructure de messagerie de votre entreprise, à simplifier la gestion du flux de messagerie et à rationaliser le contrôle de conformité des e-mails. Il s'intègre à votre infrastructure existante, peut connecter différentes applications professionnelles et automatise le traitement des e-mails entrants. Mail Manager constitue également une première ligne de défense pour le maintien d'un système de messagerie sain en gérant efficacement votre trafic de courrier électronique et en améliorant la conformité grâce à sa capacité d'archivage des e-mails.

Outre les fonctionnalités actuelles d'Amazon SES, Mail Manager comprend les fonctionnalités suivantes qui prennent en charge le trafic entrant :

- Point de terminaison d'entrée : composant clé de l'infrastructure qui utilise des politiques de filtrage et des règles que vous pouvez configurer pour déterminer quels e-mails doivent être autorisés à entrer dans votre organisation et lesquels doivent être rejetés.
- Politiques de trafic et ensembles de règles : permettez aux administrateurs de messagerie de définir et d'appliquer des règles de gestion du trafic de courrier entrant grâce à des politiques et des règles hautement personnalisables qui peuvent trier, classer, hiérarchiser et exécuter des actions sur les e-mails en fonction d'un ensemble complet de conditions et d'exceptions que vous définissez. Ce filtrage intelligent combiné à des flux de travail automatisés permet de rationaliser la gestion des e-mails, d'améliorer l'efficacité et de garantir la conformité avec les politiques de courrier électronique de votre organisation.
- Relais SMTP : redirige le trafic e-mail vers d'autres serveurs SMTP en fonction des critères que vous définissez dans les règles en connectant les systèmes de messagerie internes, et rationalise la gestion des e-mails grâce au transfert automatique. La capacité de répartir le trafic sur plusieurs serveurs et passerelles permet à votre entreprise de gérer efficacement un volume élevé de courrier électronique, même dans des environnements hybrides.
- Archivage des e-mails : enregistre et protège vos e-mails en stockant les données dans un stockage permanent et sécurisé à long terme, et vous permet de rechercher et d'archiver rapidement les e-mails. Il fournit un archivage à plein temps au niveau de l'entreprise sans augmenter les exigences de stockage de votre serveur de boîtes aux lettres.
- Compléments pour les e-mails : ensemble d'outils de sécurité spécialisés fournis par des fournisseurs approuvés par SES, qui peuvent être utilisés pour gérer les e-mails entrant dans votre terminal d'entrée et pour fournir des options de routage en fonction des résultats de sécurité. Ces outils sont des solutions certifiées de renseignement de sécurité et d'application de la loi qui sont

prêtes à être intégrées à votre flux de travail de messagerie et peuvent être activées directement depuis la console Mail Manager.

Commencer à utiliser Mail Manager

Pour commencer à utiliser Mail Manager, un assistant d'intégration dans la console Amazon SES vous expliquera les étapes d'activation de Mail Manager pour votre compte. veuillez consulter the section called “Premiers pas”.

Rubriques

Commencer à utiliser Mail Manager

Pour commencer à utiliser Amazon SES Mail Manager, vous pouvez utiliser l'assistant Get Started with Mail Manager de la console Amazon SES, où vous allez créer un point de terminaison d'entrée et le configurer avec une politique de trafic et un ensemble de règles.

Un point de terminaison d'entrée est le premier élément de base de la configuration de Mail Manager. Il s'agit d'un composant clé de l'infrastructure qui utilise :

- Politiques de trafic : une politique de trafic contient des déclarations de politique que vous définissez pour trier le courrier entrant en autorisant ou en bloquant certains types d'e-mails lorsque les conditions de la déclaration de politique sont remplies.
- Ensembles de règles : un ensemble de règles contient des règles que vous définissez pour effectuer des actions sur le courrier électronique que vous autorisez à entrer lorsque les conditions de la règle sont remplies.

Cependant, la création d'un point de terminaison d'entrée consiste notamment à sélectionner une politique de trafic et un ensemble de règles déjà créés, puis à les attribuer au point de terminaison d'entrée. Les étapes de la procédure suivante vous guideront dans le bon ordre de configuration de votre premier point de terminaison d'entrée.

Commencer à utiliser Mail Manager à l'aide de la console SES

La procédure suivante explique comment démarrer avec Mail Manager à l'aide de la console SES.

Pour démarrer avec Mail Manager à l'aide de la console Amazon SES

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation de gauche, choisissez Mail Manager et sélectionnez l'un des boutons Commencer avec Mail Manager sur la page d'aperçu du Mail Manager.
3. Sur la page Configurer, sélectionnez Créer une politique de trafic sur la carte Créer une politique de trafic.

    a. Terminez le flux de travail sur la page Créer une politique de trafic. Si vous avez besoin d'informations supplémentaires, consultezthe section called “Création de politiques de trafic et de déclarations de politique (console)”.

    b. Après avoir créé votre première politique de trafic et vos premières déclarations de politique, utilisez le bouton de retour de votre navigateur pour revenir à la page Configurer ou sélectionnez Configurer sous Gestionnaire de courrier dans le panneau de navigation de gauche.
4. Sur la page Configurer, sélectionnez Créer un ensemble de règles sur la carte Créer un ensemble de règles.

    a. Terminez le flux de travail sur la page Créer un ensemble de règles. Si vous avez besoin d'informations supplémentaires, consultezthe section called “Création d'ensembles de règles et de règles (console)”.

    b. Après avoir créé votre premier ensemble de règles et vos premières règles, utilisez le bouton de retour de votre navigateur pour revenir à la page Configurer ou sélectionnez Configurer sous Gestionnaire de courrier dans le panneau de navigation de gauche.
5. Maintenant que vous avez créé votre première politique de trafic et votre premier ensemble de règles, vous serez en mesure de créer votre premier point de terminaison d'entrée. Sur la page

Configurer, sélectionnez Créer un point de terminaison d'entrée sur la carte Créer un point de terminaison d'entrée.

- Une partie du flux de travail sur la page du point de terminaison d'entrée d'e-mails consistera à attribuer la politique de trafic et l'ensemble de règles que vous venez de créer au point de terminaison d'entrée. Si vous avez besoin d'informations supplémentaires, consultezthe section called “Création d'un point de terminaison d'entrée (console)”.

Une fois votre premier point de terminaison d'entrée créé, vous pouvez commencer à utiliser Mail Manager et utiliser ses autres fonctionnalités telles que les relais SMTP et l'archivage des e-mails. Vous pouvez également créer des points de terminaison d'entrée supplémentaires avec des politiques de trafic et des ensembles de règles uniques pour personnaliser davantage la façon dont vous gérez tous vos e-mails entrants.

Points de terminaison d'entrée

Un point de terminaison d'entrée est le principal composant de l'infrastructure de Mail Manager qui reçoit, achemine et gère vos e-mails en utilisant des politiques et des règles que vous configurez pour déterminer quels e-mails doivent être rejetés, lesquels doivent être autorisés et lesquels doivent être traités.

Chaque point de terminaison d'entrée possède sa propre politique de trafic pour déterminer les e-mails à bloquer ou à autoriser, et son propre ensemble de règles pour effectuer des actions sur le courrier électronique que vous autorisez à entrer. Par conséquent, en créant plusieurs points de terminaison d'entrée, vous pouvez déléguer chacun d'entre eux pour gérer et acheminer des types spécifiques d'e-mails. Ce niveau de granularité vous aidera à créer un système de gestion des e-mails adapté aux besoins de votre entreprise.

Flux de travail prérequis pour créer un point de terminaison d'entrée

Au moment de créer votre point de terminaison d'entrée, vous devez lui attribuer une politique de trafic et un ensemble de règles déjà créés. Par conséquent, le flux de travail pour créer un point de terminaison d'entrée doit être dans l'ordre suivant :

1. Commencez par créer une politique de trafic pour déterminer le courrier électronique que vous souhaitez bloquer ou autoriser. Pour plus de détails, consultez the section called “Création de politiques de trafic et de déclarations de politique (console)”.

2. Créez ensuite un ensemble de règles pour effectuer des actions sur le courrier électronique que vous autorisez à entrer. Pour plus de détails, consultez the section called “Création d'ensembles de règles et de règles (console)”.
3. Enfin, créez votre point de terminaison d'entrée et attribuez-lui la politique de trafic et l'ensemble de règles que vous venez de créer ou tout autre que vous avez créé précédemment.

Une fois que vous avez créé votre point de terminaison d'entrée, vous devez le configurer avec l'environnement que vous utilisez pour recevoir des e-mails, qu'il s'agisse de la configuration d'un client SMTP sur site ou d'un hôte de domaine DNS basé sur le Web. Ceci est discuté ci-dessous dansthe section called “Configuration de votre environnement ”.

Configuration de votre environnement pour utiliser un point de terminaison d'entrée

Utilisation de l'enregistrement « A »

Lorsque vous créez un point de terminaison d'entrée, un enregistrement « A » pour le point de terminaison est généré et sa valeur est affichée sur l'écran récapitulatif du point de terminaison d'entrée dans la console SES. La façon dont vous utilisez la valeur de cet enregistrement dépend du type de point de terminaison que vous avez créé et de votre cas d'utilisation :

- Point de terminaison ouvert : le courrier envoyé à votre domaine sera résolu directement vers votre point de terminaison d'entrée, aucune authentification n'est requise.
  - Copiez et collez la valeur de l'enregistrement « A » soit directement dans la configuration SMTP d'un client SMTP sur site, soit dans un enregistrement MX pour votre domaine dans votre configuration DNS.
- Point de terminaison authentifié : le courrier envoyé à votre domaine doit provenir d'expéditeurs autorisés avec lesquels vous avez partagé vos informations d'identification SMTP, tels que vos serveurs de messagerie sur site.
  - Copiez et collez la valeur de l'enregistrement « A » directement dans la configuration SMTP d'un client SMTP sur site, ainsi que votre nom d'utilisateur et votre mot de passe.

Si vous utilisez un enregistrement MX dans votre configuration, n'oubliez pas que même si chaque fournisseur DNS dispose de procédures et d'interfaces différentes pour configurer les enregistrements, les informations clés que vous devez saisir dans vos paramètres DNS sont répertoriées dans l'exemple suivant :

Tous les e-mails envoyés à recipient@marketing.example.com seront envoyés à votre point de terminaison d'entrée car vous avez saisi l'enregistrement « A » du point de terminaison d'entrée comme valeur d'un enregistrement MX dans les paramètres DNS de votre domaine :

- Domaine — `marketing.example.com`
- Valeur d'enregistrement MX — `890123abcdef.ghijk.mail-manager-smtp.amazonaws.com` (Il s'agit de la valeur d'enregistrement « A » copiée depuis votre point de terminaison d'entrée.)
- Priorité — `10`

La procédure décrite dans la section suivante vous expliquera comment créer un point de terminaison d'entrée dans la console SES.

Création d'un point de terminaison d'entrée dans la console SES

La procédure suivante explique comment utiliser la page de point de terminaison d'entrée de la console SES pour créer des points de terminaison d'entrée et gérer ceux que vous avez déjà créés.

Pour créer et gérer les points de terminaison d'entrée à l'aide de la console

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation de gauche, choisissez Ingress endpoints sous Mail Manager.
3. Sur la page des points de terminaison d'entrée, sélectionnez Créer un point de terminaison d'entrée.
4. Sur la page Créer un nouveau point de terminaison d'entrée, entrez un nom unique pour votre point de terminaison d'entrée.
5. Choisissez s'il s'agira d'un point de terminaison ouvert ou authentifié.

    - Si vous choisissez Authentifié, sélectionnez soit un mot de passe SMTP et saisissez-en un, soit Secret et sélectionnez l'un de vos secrets dans Secret ARN. Si vous sélectionnez un secret créé précédemment, il doit contenir les politiques indiquées dans les étapes suivantes pour créer un nouveau secret.
    - Vous avez la possibilité de créer un nouveau secret en choisissant Créer un nouveau. La AWS Secrets Manager console s'ouvre et vous pouvez continuer à créer une nouvelle clé :

    a. Choisissez Autre type de secret dans Type de secret.

b. Dans Paire clé/valeur, entrez `password` la clé et votre mot de passe réel pour la valeur.

> **Note**
>
> Pour Key, vous devez uniquement entrer `password` (tout le reste entraînera l'échec de l'authentification).

c. Sélectionnez Ajouter une nouvelle clé pour créer une clé gérée par le client KMS (CMK) dans Clé de chiffrement. La AWS KMS console s'ouvre.

d. Choisissez Créer une clé sur la page Clés gérées par le client.

e. Conservez les valeurs par défaut sur la page de configuration clé et sélectionnez Suivant.

f. Entrez le nom de votre clé dans Alias (vous pouvez éventuellement ajouter une description et un tag), puis dans Suivant.

g. Sélectionnez les utilisateurs (autres que vous-même) ou les rôles que vous souhaitez autoriser à administrer la clé dans Administrateurs clés, puis sur Suivant.

h. Sélectionnez les utilisateurs (autres que vous-même) ou les rôles que vous souhaitez autoriser à utiliser la clé dans Utilisateurs clés, puis Suivant.

i. Copiez-le et collez-le Politique KMS CMK dans l'éditeur de texte JSON Key policy au `"statement"` niveau en l'ajoutant sous forme d'instruction supplémentaire séparée par une virgule. Remplacez la région et le numéro de compte par les vôtres.

j. Choisissez Finish (Terminer).

k. Sélectionnez l'onglet de votre navigateur dans lequel vous avez ouvert la page AWS Secrets Manager Enregistrer un nouveau secret et sélectionnez l'icône d'actualisation (flèche circulaire) à côté du champ Clé de chiffrement, puis cliquez dans le champ et sélectionnez la clé que vous venez de créer.

l. Entrez un nom dans le champ Nom du secret de la page Configurer le secret.

m. Sélectionnez Modifier les autorisations dans Autorisations relatives aux ressources.

n. Copiez-collez le Politique en matière de ressources secrètes dans l'éditeur de texte JSON Resource Permissions et remplacez la région et le numéro de compte par les vôtres. (Assurez-vous de supprimer tout exemple de code dans l'éditeur.)

o. Choisissez Enregistrer, puis Suivant.

p. Configurez éventuellement la rotation suivie de Next.

q. Passez en revue et enregistrez votre nouveau secret en choisissant Store.

r. Sélectionnez l'onglet de votre navigateur où la page SES Create new ingress endpoint est ouverte et choisissez Actualiser la liste, puis sélectionnez le secret que vous venez de créer dans Secret ARN.

6. Sélectionnez une politique de trafic pour déterminer le courrier électronique que vous souhaitez bloquer ou autoriser.
7. Sélectionnez un ensemble de règles contenant les actions de règles que vous souhaitez effectuer sur l'e-mail que vous autorisez à entrer.
8. Sélectionnez Créer un point de terminaison d'entrée.
9. Dans Informations générales, « Provisioning » sera affiché lors de la création de votre point de terminaison d'entrée. Actualisez la page jusqu'à ce que « Actif » apparaisse et que le champ ARecord contienne une valeur. Copiez la valeur d'enregistrement « A » et collez-la dans votre configuration DNS ou dans votre client SMTP comme indiqué dansConfiguration de votre environnement .
10. Vous pouvez consulter et gérer les points de terminaison d'entrée que vous avez déjà créés à partir de la page des points de terminaison d'entrée. Si vous souhaitez supprimer un point de terminaison d'entrée, sélectionnez son bouton radio puis Supprimer.
11. Pour modifier un point de terminaison d'entrée, sélectionnez son nom pour ouvrir sa page de résumé :

    - Vous pouvez modifier le statut actif du terminal en choisissant Modifier dans les détails généraux, puis Enregistrer les modifications.
    - Vous pouvez sélectionner un ensemble de règles ou une autre politique de trafic en choisissant Modifier dans le jeu de règles ou Politique de trafic, puis Enregistrer les modifications.

Politiques de circulation et déclarations de politique

Une politique de trafic est un conteneur pour les déclarations de politique que vous attribuez à un point de terminaison d'entrée afin qu'il puisse trier le courrier entrant en autorisant ou en bloquant certains types d'e-mails lorsque les conditions des déclarations de politique sont remplies. Une politique de trafic peut être utilisée par plusieurs points de terminaison d'entrée.

> **Tip**
>
> Vous pouvez considérer une politique de trafic comme un « ensemble de filtres » et une déclaration de politique comme un « filtre ». La politique de trafic (ensemble de filtres) contient des politiques (filtres) que vous utilisez pour filtrer le courrier entrant.

Lorsque vous créez une politique de trafic, vous avez la possibilité de définir une taille de message maximale (en octets). Lorsqu'un message dépasse cette taille, il est immédiatement supprimé. Il agit comme un filtre de « premier passage » lorsqu'il est défini. Ensuite, vous définissez l'action par défaut pour autoriser ou bloquer les e-mails non conformes aux conditions de vos déclarations de politique. Imaginez cela comme une action « catch all » dans le cadre de la politique de trafic.

Les déclarations de politique sont également créées à l'aide d'une action d'autorisation ou de blocage prise lorsque les conditions des déclarations sont remplies. Vous créez les conditions en sélectionnant un protocole de courrier électronique et un opérateur conditionnel pour une valeur que vous entrez et qui doit correspondre au message entrant avant que la déclaration de politique ne l'autorise ou ne le bloque. Chaque déclaration de politique peut comporter plusieurs conditions.

Une politique de trafic peut contenir plusieurs déclarations de politique et les exécuter dans un ordre basé sur la hiérarchie implicite de la façon dont elle évalue le courrier électronique :

- Taille maximale des messages : si ce paramètre facultatif est défini, tout message supérieur à cette taille est immédiatement supprimé, sans tenir compte des déclarations de politique.
- Déclarations de politique qui bloquent : ces instructions sont évaluées en premier et bloquent tout message répondant aux conditions de la déclaration.
- Déclarations de politique autorisant — Ces déclarations sont ensuite évaluées et autorisent tout message répondant aux conditions de la déclaration.
- Action par défaut de la politique de trafic : les autres messages ne relevant pas des déclarations de politique sont autorisés ou bloqués en fonction de la manière dont vous avez défini ce paramètre.

Une politique de trafic est une ressource indépendante qui peut être utilisée par plusieurs points de terminaison d'entrée, mais les déclarations de politique appartiennent exclusivement à la politique de trafic dans laquelle elles ont été créées. Ainsi, vous devez d'abord créer une politique de trafic, ou modifier une politique existante, avant de pouvoir créer des déclarations de politique pour évaluer le courrier électronique entrant dans votre point de terminaison d'entrée.

La procédure de la section suivante explique comment créer des politiques de trafic et leurs déclarations de politique dans la console SES.

Création de politiques de trafic et de déclarations de politique dans la console SES

La procédure suivante explique comment utiliser la page Règles de trafic de la console SES pour créer des politiques de trafic et leurs déclarations de politique, et gérer celles que vous avez déjà créées.

Pour créer et gérer des politiques de trafic et des déclarations de politique à l'aide de la console

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation de gauche, choisissez Politiques de trafic sous Mail Manager.
3. Sur la page Politiques de trafic, sélectionnez Créer une politique de trafic.
4. Sur la page Créer une politique de trafic, entrez un nom unique pour votre politique de trafic.
5. (Facultatif) Si vous souhaitez supprimer les messages dépassant une certaine taille, entrez une valeur en octets dans le champ Taille maximale des messages.
6. Dans Action par défaut, choisissez si la politique de trafic consiste à autoriser ou à refuser (bloquer) les messages qui ne respectent pas (ne sont pas pris en compte) les conditions de vos déclarations de politique.
7. Sélectionnez Ajouter une nouvelle déclaration de politique pour créer une déclaration pour votre politique de trafic.
8. Choisissez Autoriser ou Refuser (bloquer) pour que l'action soit entreprise lorsque les conditions de l'instruction sont remplies.
9. Créez une condition en sélectionnant un protocole de courrier électronique et un opérateur conditionnel pour la valeur que vous entrez. Sélectionnez Ajouter une nouvelle condition si vous souhaitez ajouter d'autres conditions à cette déclaration de politique. Pour en savoir plus sur une propriété de condition, ses opérateurs et ses valeurs valides, consultez la référence des conditions de la déclaration de politique.

    - Si vous êtes abonné à un module complémentaire de messagerie, vous pourrez le sélectionner ici en tant que protocole de courrier électronique.
10. Si vous souhaitez ajouter d'autres déclarations de politique et conditions, répétez les étapes 7 à 9 ci-dessus.

11. Lorsque vous avez terminé de créer les déclarations de politique et leurs conditions, sélectionnez Créer une politique de trafic.
12. Vous pouvez consulter et gérer les politiques de trafic que vous avez déjà créées à partir de la page Politiques de trafic. Si vous souhaitez supprimer une politique de trafic, sélectionnez son bouton radio, puis Supprimer.
13. Pour modifier les propriétés d'une politique de trafic ou l'une de ses déclarations de politique, sélectionnez son nom pour ouvrir sa page d'aperçu, puis sélectionnez Modifier.
14. Dans les détails de la politique de trafic, vous pouvez modifier la taille maximale des messages et l'action par défaut.
15. Dans tous les conteneurs de déclarations de politique, vous pouvez modifier la propriété autoriser/refuser et modifier toutes les conditions. Vous pouvez également supprimer des déclarations de politique et des conditions, ainsi qu'en ajouter de nouvelles.
16. Lorsque vous avez terminé toutes vos modifications, enregistrez-les en sélectionnant Enregistrer les modifications.

Référence pour les conditions de la déclaration de politique

Conditions de la déclaration de politique

Le tableau de référence suivant répertorie tous les protocoles de déclaration de politique disponibles pour créer une condition de déclaration de politique. La sélection du type d'expression d'un protocole vous amène à sa page de référence dans le manuel de référence de l'API SES Mail Manager qui répertorie tous les opérateurs disponibles et les valeurs valides pour ce protocole.

Conditions de l'énoncé de politique : protocoles, opérateurs et valeurs

Protocole	Type d'expression
Adresse du destinataire	Opérateurs et valeurs valides pour les expressions de chaîne
Plage d'adresses IP de l'expéditeur	Opérateurs et valeurs valides pour les expressions IP
Version du protocole TLS	Opérateurs et valeurs valides pour les expressions du protocole TLS

Protocole	Type d'expression
Abusix Mail Intelligence (si vous êtes abonné) Liste de domaines bloqués Spamhaus (si abonné)	Opérateurs et valeurs valides pour les expressions booléennes

Ensembles de règles et règles

Les ensembles de règles sont des conteneurs pour les règles que vous attribuez à un point de terminaison d'entrée afin qu'il puisse effectuer des actions sur les e-mails autorisés à entrer conformément à la politique de trafic du point de terminaison d'entrée. Un ensemble de règles peut être utilisé par plusieurs points de terminaison d'entrée.

Les règles indiquent à votre point de terminaison d'entrée comment gérer les e-mails entrants en exécutant les actions définies dans la règle lorsque les messages répondent aux conditions de la règle. Chaque règle peut comporter plusieurs conditions et actions. Les règles que vous créez dans un ensemble de règles sont exécutées dans l'ordre que vous spécifiez dans l'ensemble de règles.

Vous définissez les conditions de la règle en sélectionnant une propriété d'e-mail et un opérateur conditionnel pour une valeur que vous entrez et qui doit correspondre au message avant que la règle n'exécute ses actions. Vous définissez les actions à effectuer ainsi que leur ordre d'exécution.

Pour une plus grande granularité, vos règles peuvent également contenir des exceptions définies de la même manière que des conditions, mais vous définissez ici une condition à laquelle le message ne doit pas correspondre. Les conditions et les exceptions fonctionnent indépendamment. Vous pouvez créer une règle avec uniquement des exceptions si vous le souhaitez, ainsi que des conditions et des exceptions de mixage.

En raison de la fine granularité de la manière dont les règles peuvent être définies au sein d'un ensemble de règles, la liste suivante est fournie pour illustrer la relation entre les composants d'un ensemble de règles :

- Les ensembles de règles contiennent :
  - Règles : vous pouvez définir l'ordre dans lequel les règles sont exécutées au sein de l'ensemble de règles.

    Les règles contiennent :

- Conditions — La règle s'applique si le message correspond à l'évaluation des conditions ; et si la règle comporte des exceptions, voir ci-dessous.
- Exceptions — La règle s'applique si le message ne correspond pas à l'évaluation des exceptions ; et si la règle comporte des conditions, voir ci-dessus.
- Actions : les actions sont déclenchées lorsque la règle s'applique : toutes les conditions sont réunies, aucune exception n'est prévue.

  Vous pouvez définir l'ordre dans lequel les actions sont exécutées dans le cadre de la règle.

Étant donné que chaque règle peut comporter plusieurs conditions, exceptions et actions, et que vous pouvez définir l'ordre dans lequel les règles et les actions sont exécutées, cela vous permet de créer une solution de gestion des e-mails très personnalisée et automatisée adaptée aux besoins spécifiques de votre entreprise.

Un ensemble de règles est une ressource indépendante qui peut être utilisée par plusieurs points de terminaison d'entrée, mais les règles appartiennent exclusivement à l'ensemble de règles dans lequel elles ont été créées. Ainsi, vous devez d'abord créer un ensemble de règles, ou modifier un ensemble existant, avant de pouvoir créer des règles pour agir sur le courrier électronique entrant dans votre point de terminaison d'entrée.

La procédure décrite dans la section suivante vous expliquera comment créer des ensembles de règles et leurs règles dans la console SES.

Création d'ensembles de règles et de règles dans la console SES

La procédure suivante explique comment utiliser la page Ensembles de règles de la console SES pour créer des ensembles de règles et leurs règles, et gérer ceux que vous avez déjà créés.

Pour créer et gérer des ensembles de règles et des règles à l'aide de la console

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation de gauche, choisissez Ensembles de règles sous Mail Manager.
3. Sur la page Ensembles de règles, choisissez Créer un ensemble de règles et entrez un nom unique pour votre ensemble de règles.
4. Sur la page d'aperçu de l'ensemble de règles, sélectionnez Modifier, puis sélectionnez Créer une nouvelle règle sur la page de modification.

5. Dans la barre latérale Détails de la règle, entrez un nom unique pour votre règle.
6. Sélectionnez Ajouter une nouvelle condition pour créer une condition à laquelle le message doit correspondre ; ou cochez la case SAUF dans le cas de : suivie de Ajouter une nouvelle exception pour créer une condition à laquelle le message ne doit pas correspondre.
7. Créez la condition ou l'exception en sélectionnant une propriété d'e-mail et un opérateur conditionnel pour la valeur que vous entrez. Sélectionnez Ajouter une nouvelle condition ou Ajouter une nouvelle exception si vous souhaitez ajouter d'autres conditions ou exceptions à cette règle. Pour en savoir plus sur une propriété de condition, ses opérateurs et ses valeurs valides, consultez la référence des conditions de règle.

   - Si vous êtes abonné à un module complémentaire d'e-mail, vous pourrez le sélectionner ici en tant que propriété d'e-mail.
8. Sélectionnez Ajouter une nouvelle action pour définir l'action à entreprendre lorsque les conditions de la règle sont réunies et/ou que les exceptions ne correspondent pas. Pour ajouter d'autres actions à effectuer, sélectionnez Ajouter une nouvelle action. Pour en savoir plus sur les actions et leurs paramètres, consultez la référence des actions des règles.

   - Pour exécuter les actions de règle Écrire dans S3, Envoyer dans la boîte aux lettres et Envoyer vers Internet, vous devez avoir Politiques d'action relatives aux règles activé la règle pour votre compte ; sinon, l'action de la règle échouera.
   - Lorsque vous créez deux actions ou plus, des flèches haut/bas s'affichent pour vous permettre de définir l'ordre d'exécution.
9. Lorsque vous avez fini de créer les conditions, les exceptions et les actions de la règle, vous l'enregistrez dans son ensemble de règles en choisissant Enregistrer le jeu de règles situé dans le panneau Modifier l'ensemble de règles sur la gauche.
10. Si vous souhaitez ajouter d'autres règles à l'ensemble de règles, répétez les étapes 4 à 9 ci-dessus.

    - Lorsque vous créez deux règles ou plus, des flèches haut/bas sont affichées dans la colonne Réorganiser de l'ensemble de règles afin que vous puissiez définir l'ordre d'exécution.
11. Vous pouvez consulter et gérer les ensembles de règles que vous avez déjà créés à partir de la page Ensembles de règles. Si vous souhaitez supprimer un ensemble de règles, sélectionnez son bouton radio puis Supprimer.
12. Pour modifier un ensemble de règles, sélectionnez son nom pour ouvrir sa page d'aperçu. À partir de là, sélectionnez Modifier pour réorganiser l'exécution de ses règles, ajouter d'autres

règles en choisissant Créer une nouvelle règle ou supprimer une règle en sélectionnant son bouton radio suivi de Supprimer.

13. Pour modifier une règle, sélectionnez son bouton radio. Dans tous les conteneurs de la barre latérale Détails des règles, vous pouvez modifier toutes les conditions ou exceptions et modifier ou réorganiser toutes les actions. Vous pouvez également supprimer des conditions, des exceptions et des actions, ainsi qu'en ajouter de nouvelles.
14. Lorsque vous avez terminé toutes vos modifications, enregistrez vos modifications en sélectionnant Enregistrer l'ensemble de règles dans le panneau Modifier l'ensemble de règles sur la gauche.

Référence pour les règles, les conditions et les actions

Conditions du règlement

Le tableau de référence suivant répertorie toutes les propriétés de règle disponibles pour créer une condition de règle (ou une exception) et qui sont classées par type d'expression. Les propriétés de règle qui partagent le même type d'expression partagent également les mêmes opérateurs et valeurs. La sélection du type d'expression d'une propriété vous amène à sa page de référence dans le manuel de référence de l'API SES Mail Manager qui répertorie tous les opérateurs disponibles et les valeurs valides pour cette propriété.

Conditions des règles : propriétés, opérateurs et valeurs

Propriété	Type d'expression
Depuis l'adresse	Opérateurs et valeurs valides pour les expressions de chaîne
À adresser	
Adresse CC	
Courrier de	
Adresse du destinataire	
Sujet	
Bonjour	

Propriété	Type d'expression
plage IP	Opérateurs et valeurs valides pour les expressions IP
Taille maximale du message	Opérateurs et valeurs valides pour les expressions numériques
DKIM SPF Analyse antivirus Trend Micro (si vous êtes abonné)	Opérateurs et valeurs valides pour les expressions de verdict
TLS Enveloppé en TLS Lire le reçu	Opérateurs et valeurs valides pour les expressions booléennes
Politique DMARC	Opérateurs et valeurs valides pour les expressions DMARC

Actions relatives aux règles

Le tableau de référence suivant répertorie toutes les actions de règle qui peuvent être entreprises lorsque les conditions d'une règle sont remplies ou que ses exceptions ne le sont pas. En sélectionnant une action, vous serez redirigé vers la page de référence de l'action dans le manuel de référence de l'API SES Mail Manager qui répertorie les paramètres et leurs formats pour l'action. Le tableau utilise les noms d'action adoptés dans la console Mail Manager ; les noms des API peuvent être légèrement différents.

> **Note**
>
> Dans certaines références d'API, un *`ActionFailurePolicy`* paramètre peut être défini sur Continue ou Drop en cas d'échec de l'action. Cela ne s'applique que lors de l'utilisation de l'API ; lors de l'utilisation de la console, la valeur par défaut de Continue *`ActionFailurePolicy`* a été définie sur Continue.

Actions liées aux règles : actions et paramètres

Les actions et leurs paramètres	Description
Ecrire à S3	Écrit le contenu MIME de l'e-mail dans un compartiment S3.
Action de relais SMTP	Relaie l'e-mail via SMTP vers un autre serveur SMTP spécifique.
Action d'archivage	Archive l'e-mail en le transférant vers une archive Amazon SES.
Ajouter un en-tête	Ajoute un en-tête personnalisé à l'e-mail reçu.
Réécriture des destinataires des e-mails	Remplace les destinataires de l'enveloppe e-mail par la liste de destinataires donnée. Si la condition de cette action s'applique uniquement à un sous-ensemble de destinataires, seuls ces destinataires sont remplacés.
Livrer dans une boîte aux lettres	Envoie l'e-mail dans une WorkMail boîte aux lettres Amazon.
Envoyer vers Internet	Utilise SES pour envoyer l'e-mail au (x) destinataire (s) figurant sur la liste des destinataires de l'e-mail.
Action de suppression	Pour les e-mails comportant plusieurs destinataires, si cette action s'applique à un ou plusieurs (mais pas à tous) de ces destinataires, ils seront supprimés de la liste des destinataires de l'e-mail et le traitement continu des règles s'appliquera aux destinataires restants. Si cette action s'applique à tous les destinataires, le traitement des règles s'arrête car tous les destinataires sont supprimés de la liste des destinataires et ne recevront pas l'e-mail.

relais SMTP

Mail Manager étant déployé entre votre environnement de messagerie (tel que Microsoft 365, Google Workspace ou On-Premise Exchange) et Internet, Mail Manager utilise des relais SMTP pour acheminer les e-mails entrants traités par Mail Manager vers votre environnement de messagerie. Il peut également acheminer les e-mails sortants vers une autre infrastructure de messagerie telle qu'un autre serveur Exchange ou une passerelle de messagerie tierce avant de les envoyer aux destinataires finaux.

Un relais SMTP est un composant essentiel de votre infrastructure de messagerie, chargé de router efficacement les e-mails entre les serveurs lorsqu'il est désigné par une action de règle définie dans un ensemble de règles.

Plus précisément, un relais SMTP peut rediriger le courrier entrant entre SES Mail Manager et une infrastructure de messagerie externe telle qu'Exchange, des passerelles de messagerie sur site ou tierces, etc. Les e-mails entrants destinés à un point de terminaison d'entrée seront traités par une règle qui acheminera les e-mails spécifiés vers le relais SMTP désigné, qui les transmettra à son tour à l'infrastructure de messagerie externe définie dans le relais SMTP.

Lorsque votre point de terminaison d'entrée reçoit des e-mails, il utilise une politique de trafic pour déterminer les e-mails à bloquer ou à autoriser. L'e-mail que vous autorisez à entrer est transmis à un ensemble de règles qui applique des règles conditionnelles pour exécuter les actions que vous avez définies pour des types d'e-mails spécifiques. L'une des actions de règle que vous pouvez définir est l'action SMTPRelay. Si vous sélectionnez cette action, l'e-mail sera transmis au serveur SMTP externe défini dans votre relais SMTP.

Par exemple, vous pouvez utiliser l'action SMTPRelay pour envoyer des e-mails depuis votre point de terminaison d'entrée vers votre serveur Microsoft Exchange sur site. Vous devez configurer votre serveur Exchange pour disposer d'un point de terminaison SMTP public accessible uniquement à l'aide de certaines informations d'identification. Lorsque vous créez le relais SMTP, vous entrez le nom du serveur, le port et les informations d'identification de votre serveur Exchange et vous attribuez à votre relais SMTP un nom unique, par exemple « »RelayToMyExchangeServer. Ensuite, vous créez une règle dans l'ensemble de règles de votre point de terminaison d'entrée qui dit : « Lorsque l'adresse d'origine contient 'gmail.com', effectuez une action SMTPRelay à l'aide du relais SMTP appelé ». RelayToMyExchangeServer

Désormais, lorsqu'un e-mail provenant de gmail.com arrive à votre point de terminaison d'entrée, la règle déclenche l'action SMTPRelay et contacte votre serveur Exchange à l'aide des informations d'identification que vous avez fournies lors de la création de votre relais SMTP et transmet le courrier

électronique à votre serveur Exchange. Ainsi, le courrier électronique reçu de gmail.com est relayé vers votre serveur Exchange.

Vous devez d'abord créer un relais SMTP avant de pouvoir le désigner dans une action de règle. La procédure décrite dans la section suivante vous expliquera comment créer un relais SMTP dans la console SES.

Création d'un relais SMTP dans la console SES

La procédure suivante explique comment utiliser la page des relais SMTP de la console SES pour créer des relais SMTP et gérer ceux que vous avez déjà créés.

Pour créer et gérer des relais SMTP à l'aide de la console

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation de gauche, choisissez Relais SMTP sous Mail Manager.
3. Sur la page des relais SMTP, sélectionnez Créer un relais SMTP.
4. Sur la page Créer un relais SMTP, entrez un nom unique pour votre relais SMTP.
5. Selon que vous souhaitez configurer un relais SMTP entrant (non authentifié) ou sortant (authentifié), suivez les instructions correspondantes :

   Inbound

   Pour configurer un relais SMTP entrant

   1. Lorsque le relais SMTP est utilisé comme passerelle entrante pour acheminer les e-mails entrants traités par Mail Manager vers votre environnement de messagerie externe, vous devez d'abord configurer l'environnement d'hébergement des e-mails. Bien que chaque fournisseur d'hébergement de messagerie dispose de sa propre interface graphique et de son propre flux de travail de configuration, les principes de configuration pour qu'ils fonctionnent avec les passerelles entrantes, telles que le relais SMTP de votre gestionnaire de courrier, seront similaires.

      Pour illustrer cela, nous avons fourni des exemples de configuration de Google Workspaces et de Microsoft Office 365 pour qu'ils fonctionnent avec votre relais SMTP en tant que passerelle entrante dans les sections suivantes :

      - Configuration de Google Workspaces

- Configuration de Microsoft Office 365

SES ne prend actuellement en charge que les relais SMTP entrants (non authentifiés) pour Google Workspaces et Microsoft Office 365.

> **Note**
>
> Assurez-vous que les domaines des destinations de destination prévues sont des identités de domaine vérifiées par SES. Par exemple, si vous souhaitez envoyer un e-mail aux destinataires abc@example.com et support@acme.com, les domaines exemple.com et acme.com doivent être vérifiés dans SES. Si le domaine d'un destinataire n'est pas vérifié, SES ne tentera pas de remettre l'e-mail au serveur SMTP public. Pour plus d'informations, consultez the section called "Création et vérification des identités".

2. Après avoir configuré Google Workspaces ou Microsoft Office 365 pour qu'ils fonctionnent avec les passerelles entrantes, entrez le nom d'hôte du serveur SMTP public avec les valeurs ci-dessous correspondant à votre fournisseur :

   - Espaces de travail Google : `aspmx.l.google.com`
   - Microsoft Office 365 : `<your_domain>.mail.protection.outlook.com`

     Remplacez les points par « - » dans votre nom de domaine. Par exemple, si votre domaine est acme.com, vous devez entrer `acme-com.mail.protection.outlook.com`

3. Entrez le numéro de port 25 pour le serveur SMTP public.
4. Laissez la section Authentification vide (ne sélectionnez ni ne créez d'ARN secret).

Outbound

Pour configurer un relais SMTP sortant

1. Entrez le nom d'hôte du serveur SMTP public auquel vous souhaitez que votre relais se connecte.
2. Entrez le numéro de port du serveur SMTP public.

3. Configurez l'authentification pour votre serveur SMTP en sélectionnant l'un de vos secrets dans Secret ARN. Si vous sélectionnez un secret créé précédemment, il doit contenir les politiques indiquées dans les étapes suivantes pour créer un nouveau secret.

   - Vous avez la possibilité de créer un nouveau secret en choisissant Créer un nouveau. La AWS Secrets Manager console s'ouvre et vous pouvez continuer à créer une nouvelle clé :

   a. Choisissez Autre type de secret dans Type de secret.

   b. Entrez les clés et valeurs suivantes dans des paires clé/valeur :

Clé	value
`username`	mon_nom d'utilisateur
`password`	mon_mot de passe

   > **Note**
   >
   > Pour les deux clés, vous devez uniquement saisir `username` et `password` comme indiqué (toute autre option entraînera l'échec de l'authentification). Pour les valeurs, entrez respectivement votre nom d'utilisateur et votre mot de passe.

   c. Sélectionnez Ajouter une nouvelle clé pour créer une clé gérée par le client KMS (CMK) dans Clé de chiffrement. La AWS KMS console s'ouvre.

   d. Choisissez Créer une clé sur la page Clés gérées par le client.

   e. Conservez les valeurs par défaut sur la page de configuration clé et sélectionnez Suivant.

   f. Entrez le nom de votre clé dans Alias (vous pouvez éventuellement ajouter une description et un tag), puis dans Suivant.

   g. Sélectionnez les utilisateurs (autres que vous-même) ou les rôles que vous souhaitez autoriser à administrer la clé dans Administrateurs clés, puis sur Suivant.

h. Sélectionnez les utilisateurs (autres que vous-même) ou les rôles que vous souhaitez autoriser à utiliser la clé dans Utilisateurs clés, puis Suivant.

i. Copiez-le et collez-le Politique KMS CMK dans l'éditeur de texte JSON Key policy au `"statement"` niveau en l'ajoutant sous forme d'instruction supplémentaire séparée par une virgule. Remplacez la région et le numéro de compte par les vôtres.

j. Choisissez Finish (Terminer).

k. Sélectionnez l'onglet de votre navigateur dans lequel vous avez ouvert la page AWS Secrets Manager Enregistrer un nouveau secret et sélectionnez l'icône d'actualisation (flèche circulaire) à côté du champ Clé de chiffrement, puis cliquez dans le champ et sélectionnez la clé que vous venez de créer.

l. Entrez un nom dans le champ Nom du secret de la page Configurer le secret.

m. Sélectionnez Modifier les autorisations dans Autorisations relatives aux ressources.

n. Copiez-collez le Politique en matière de ressources secrètes dans l'éditeur de texte JSON Resource Permissions et remplacez la région et le numéro de compte par les vôtres. (Assurez-vous de supprimer tout exemple de code dans l'éditeur.)

o. Choisissez Enregistrer, puis Suivant.

p. Configurez éventuellement la rotation suivie de Next.

q. Passez en revue et enregistrez votre nouveau secret en choisissant Store.

r. Sélectionnez l'onglet de votre navigateur où la page SES Create new ingress endpoint est ouverte et choisissez Actualiser la liste, puis sélectionnez le secret que vous venez de créer dans Secret ARN.

6. Sélectionnez Créer un relais SMTP.

7. Vous pouvez afficher et gérer les relais SMTP que vous avez déjà créés à partir de la page des relais SMTP. Si vous souhaitez supprimer un relais SMTP, sélectionnez son bouton radio puis Supprimer.

8. Pour modifier un relais SMTP, sélectionnez son nom. Sur la page de détails, vous pouvez modifier le nom du relais, le nom, le port et les informations de connexion du serveur SMTP externe en sélectionnant le bouton Modifier ou Mettre à jour correspondant, puis sur Enregistrer les modifications.

Configuration de Google Workspaces pour le relais SMTP entrant (non authentifié)

L'exemple de procédure pas à pas suivant montre comment configurer Google Workspaces pour qu'il fonctionne avec un relais SMTP entrant (non authentifié) de Mail Manager.

Prérequis

- Accès à la console d'administration Google (console d'administration Google > Applications > Google Workspace > Gmail).
- Accès au serveur de noms de domaine hébergeant les enregistrements MX pour les domaines qui seront utilisés pour la configuration de Mail Manager.

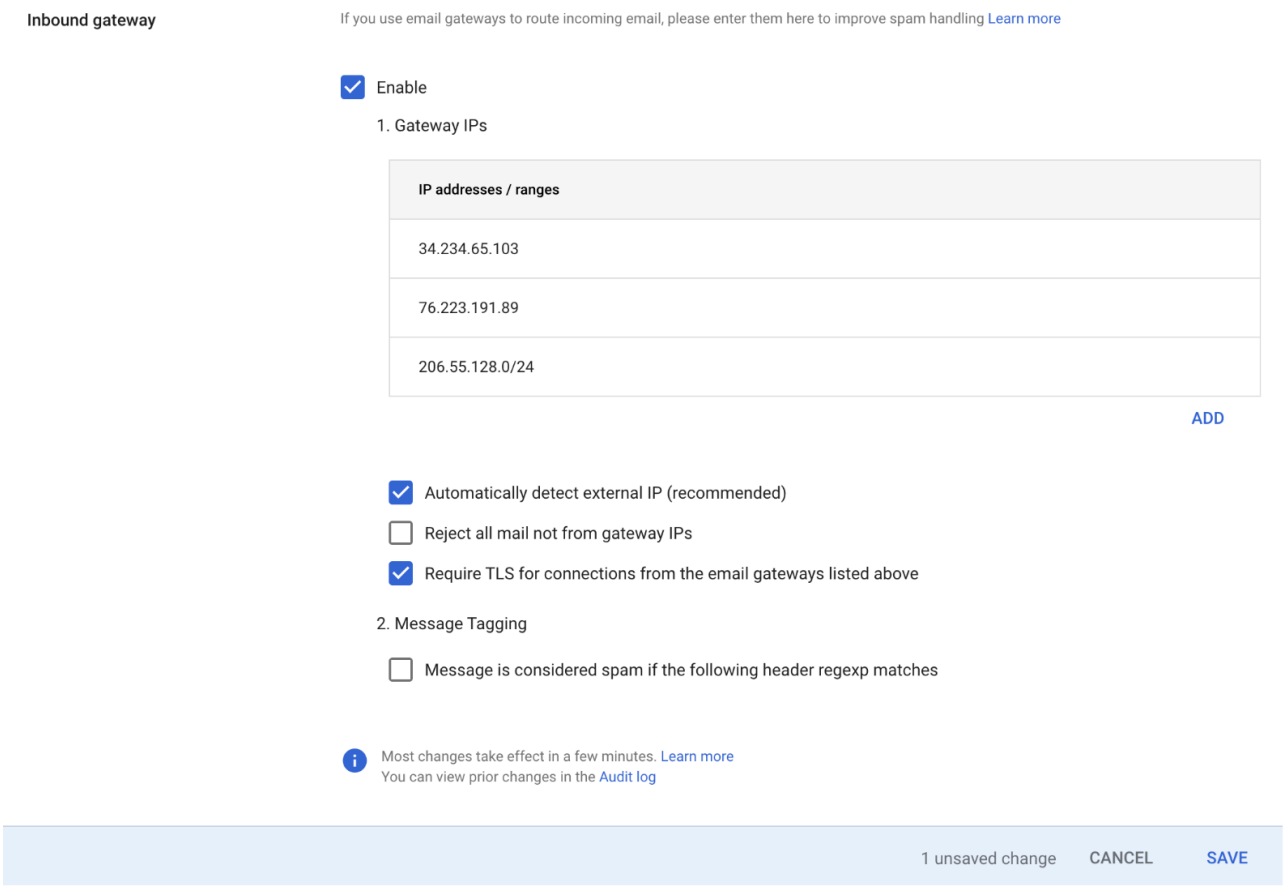
Pour configurer Google Workspaces pour qu'il fonctionne avec un relais SMTP entrant

- Ajouter les adresses IP de Mail Manager à la configuration de la passerelle entrante

  a. Dans la console d'administration Google, accédez à Applications > Google Workspace > Gmail.

  b. Sélectionnez Spam, Phishing et Malware, puis accédez à Configuration de la passerelle entrante.

  c. Activez la passerelle entrante et configurez-la avec les informations suivantes :



- Dans Gateway IPs, sélectionnez Ajouter, puis ajoutez les adresses IP des points de terminaison d'entrée spécifiques à votre région dans le tableau suivant :

Région	plage IP
UE-Ouest-1/Dub	206,55,133,0/24
EU-Central-1/FRA	206,55,132,0/24
US-Ouest-2/PDX	206,55,131,0/24
AP-Northeast-1/NRT	206,55,130,0/24
US-East-1/IAD	206,55,129,0/24
AP-Southeast-2/SYD	206,55,128,0/24

- Sélectionnez Détecter automatiquement l'adresse IP externe.

- Sélectionnez Exiger le protocole TLS pour les connexions à partir des passerelles de messagerie répertoriées ci-dessus.
- Sélectionnez Enregistrer en bas de la boîte de dialogue pour enregistrer la configuration. Une fois enregistrée, la console de l'administrateur indiquera que la passerelle entrante est activée.

Configuration de Microsoft Office 365 pour le relais SMTP entrant (non authentifié)

L'exemple de procédure pas à pas suivant vous montre comment configurer Microsoft Office 365 pour qu'il fonctionne avec un relais SMTP entrant (non authentifié) Mail Manager.

Prérequis

- Accès au centre d'administration Microsoft Security (centre d'administration Microsoft Security > Courrier électronique et collaboration > Politiques et règles > Politiques relatives aux menaces).
- Accès au serveur de noms de domaine hébergeant les enregistrements MX pour les domaines qui seront utilisés pour la configuration de Mail Manager.

Pour configurer Microsoft Office 365 pour qu'il fonctionne avec un relais SMTP entrant

1. Ajouter les adresses IP de Mail Manager à la liste des adresses autorisées

   a. Dans le centre d'administration de Microsoft Security, accédez à E-mail et collaboration > Politiques et règles > Politiques relatives aux menaces.

   b. Sélectionnez Antispam sous Politiques.

   c. Sélectionnez Politique de filtre de connexion, puis Modifier la politique de filtre de connexion.

      - Dans la boîte de dialogue Toujours autoriser les messages provenant des adresses IP ou des plages d'adresses suivantes, ajoutez les adresses IP des points de terminaison d'entrée spécifiques à votre région dans le tableau suivant :

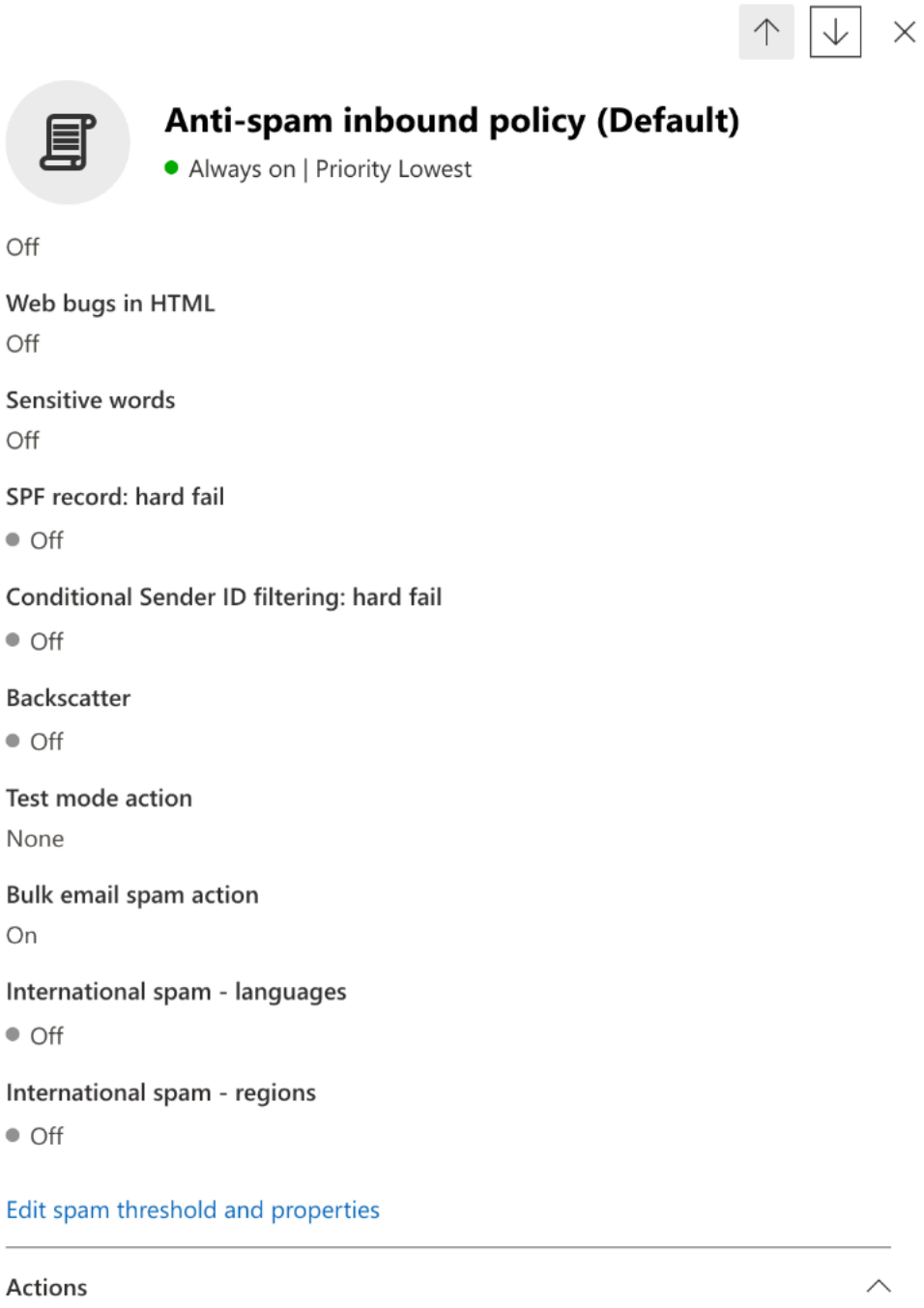
Région	plage IP
UE-Ouest-1/Dub	206,55,133,0/24

Région	plage IP
EU-Central-1/FRA	206,55,132,0/24
US-Ouest-2/PDX	206,55,131,0/24
AP-Northeast-1/NRT	206,55,130,0/24
US-East-1/IAD	206,55,129,0/24
AP-Southeast-2/SYD	206,55,128,0/24

- Sélectionnez Save.

d. Revenez à l'option Antispam et choisissez Politique anti-spam pour les envois entrants.

- Au bas de la boîte de dialogue, sélectionnez Modifier le seuil de spam et les propriétés :



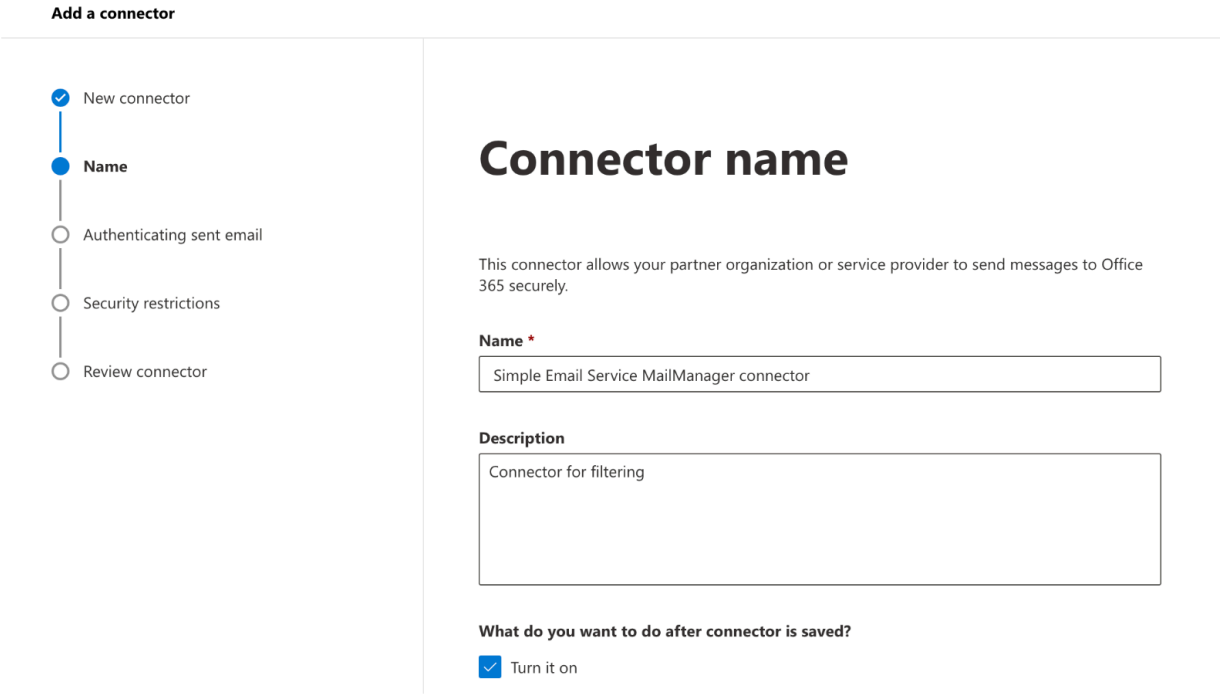
- Faites défiler la page jusqu'à Marquer comme spam et assurez-vous que l'option SPF record : hard fail est définie sur Désactivé.
- Sélectionnez Save.

2. Configuration de filtrage améliorée (recommandée)

   Cette option permettra à Microsoft Office 365 d'identifier correctement l'adresse IP de connexion d'origine avant que le message ne soit reçu par SES Mail Manager.

a. Création d'un connecteur entrant

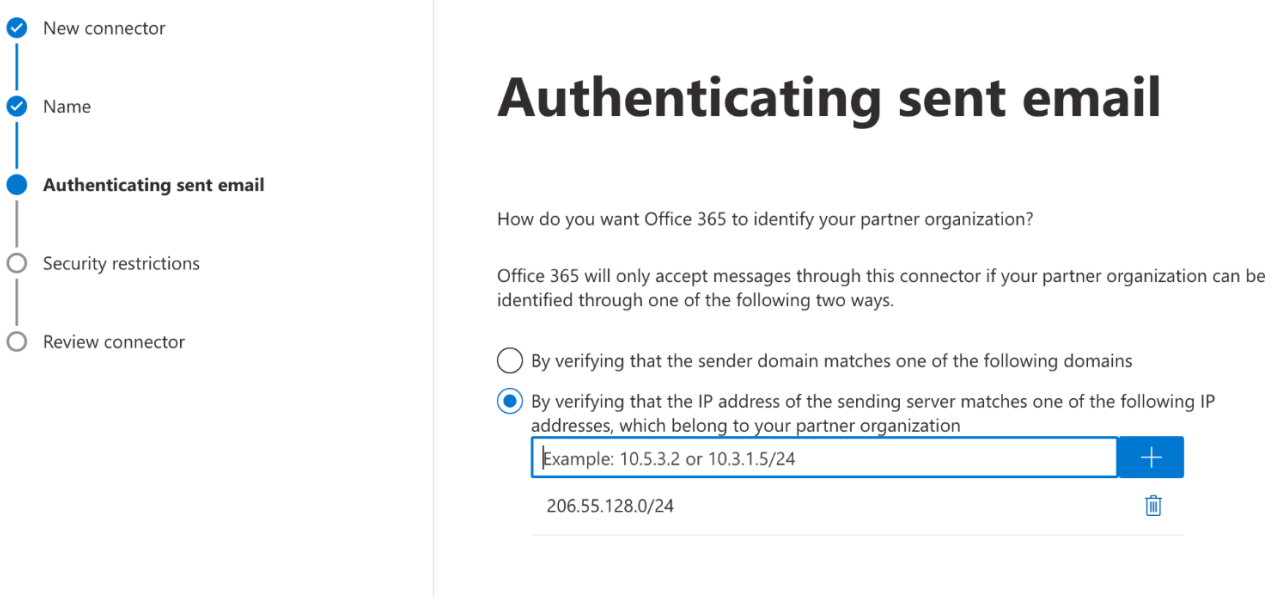
- Connectez-vous au nouveau centre d'administration Exchange et accédez à Flux de messagerie > Connecteurs.
- Sélectionnez Ajouter un connecteur.
- Dans Connection from, sélectionnez Organisation partenaire, puis Next.
- Remplissez les champs comme suit :
  - Nom — Connecteur Simple Email Service Mail Manager
  - Description — Connecteur pour le filtrage



- Sélectionnez Suivant.
- Dans Authentifier le courrier électronique envoyé, sélectionnez En vérifiant que l'adresse IP du serveur d'envoi correspond à l'une des adresses IP suivantes, qui appartient à votre organisation partenaire, puis ajoutez les adresses IP des points de terminaison d'entrée spécifiques à votre région dans le tableau suivant :

Région	plage IP
UE-Ouest-1/Dub	206,55,133,0/24

Région	plage IP
EU-Central-1/FRA	206,55,132,0/24
US-Ouest-2/PDX	206,55,131,0/24
AP-Northeast-1/NRT	206,55,130,0/24
US-East-1/IAD	206,55,129,0/24
AP-Southeast-2/SYD	206,55,128,0/24

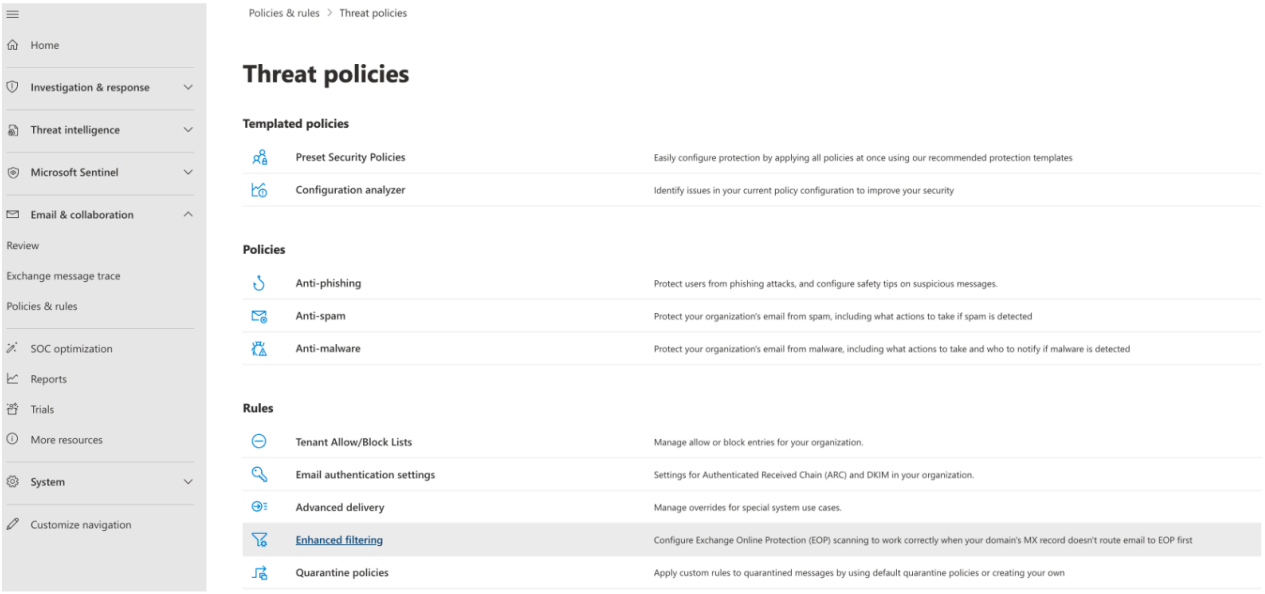


- Sélectionnez Suivant.
- Dans Restrictions de sécurité, acceptez le paramètre par défaut Rejeter les e-mails s'ils ne sont pas envoyés via le protocole TLS, puis cliquez sur Suivant.
- Vérifiez vos paramètres et sélectionnez Créer un connecteur.

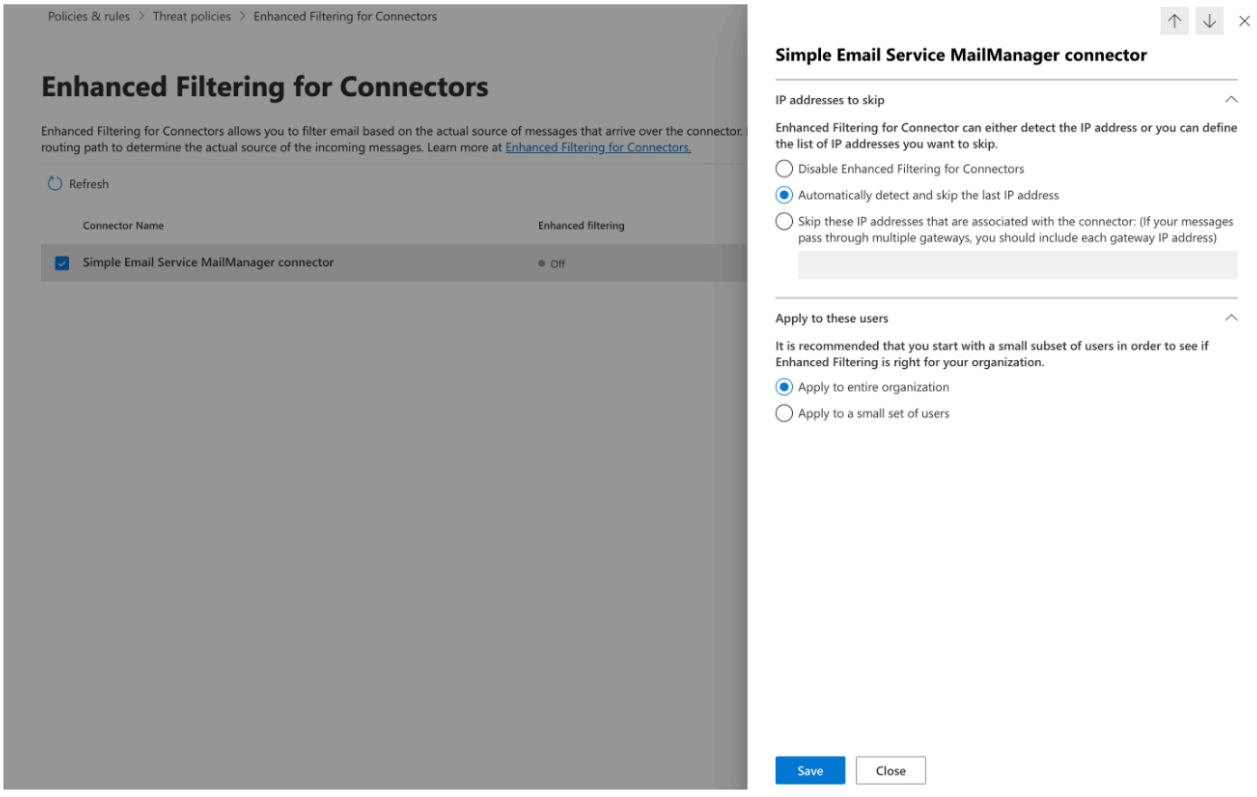
b. Activer le filtrage amélioré

Maintenant que le connecteur entrant a été configuré, vous devez activer la configuration de filtrage améliorée du connecteur dans le centre d'administration Microsoft Security.

- Dans le centre d'administration de Microsoft Security, accédez à E-mail et collaboration > Politiques et règles > Politiques relatives aux menaces.
- Sélectionnez Filtrage amélioré sous Règles.



- Sélectionnez le connecteur Simple Email Service Mail Manager que vous avez créé précédemment pour modifier ses paramètres de configuration.
- Sélectionnez à la fois Détecter automatiquement et ignorer la dernière adresse IP et Appliquer à l'ensemble de l'organisation.



- Sélectionnez Save.

Archivage des e-mails

L'archivage des e-mails vous permet d'archiver les types d'e-mails que vous spécifiez et qui entrent dans votre terminal d'entrée, ainsi que de retrouver vos messages archivés grâce à un ensemble complet de filtres de recherche avancés et à la possibilité d'exporter les résultats.

L'archivage des e-mails enregistre et protège vos e-mails en stockant les données dans un stockage permanent et sécurisé à long terme, et vous permet de rechercher et d'archiver rapidement les e-mails. Il fournit un archivage à plein temps au niveau de l'entreprise sans augmenter les exigences de stockage de votre serveur de boîtes aux lettres.

Lorsque votre point de terminaison d'entrée reçoit des e-mails, il utilise une politique de trafic pour déterminer les e-mails à bloquer ou à autoriser. L'e-mail que vous autorisez à entrer est transmis à un ensemble de règles qui applique des règles conditionnelles pour exécuter les actions que vous avez définies pour des types d'e-mails spécifiques. L'une des actions de règle que vous pouvez définir est l'action d'archivage. Si vous sélectionnez cette action, l'e-mail sera archivé dans l'archive d'e-mails que vous désignez.

Vous devez d'abord créer une archive avant de pouvoir la désigner dans une action de règle. La procédure décrite dans la section suivante vous guidera dans la création d'une archive dans la console SES.

Utilisation de l'archivage des e-mails dans la console Amazon SES

La page d'archivage des e-mails de la console SES comprend quatre tableaux interactifs, Archive de recherche, Historique des recherches, Historique des exportations et Gestion des archives, que vous pouvez utiliser pour rechercher des e-mails dans vos archives, exporter les résultats et gérer vos archives. Dans les procédures suivantes, des instructions sont fournies pour chaque table.

Pour utiliser la page d'archivage des e-mails pour rechercher, exporter et gérer vos archives

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation de gauche, choisissez Archivage des e-mails sous Mail Manager.
3. La page d'archivage des e-mails comprend quatre tableaux Archive de recherche, Historique des recherches, Historique des exportations et Gestion des archives. Pour obtenir des instructions spécifiques à chacun de ces tableaux, sélectionnez l'onglet correspondant ci-dessous :

Search archive

L'archive de recherche est un tableau interactif qui vous permet de rechercher et de retrouver vos messages archivés grâce à un filtre riche et à un ensemble de dates proposant des critères de recherche détaillés pour trouver n'importe quoi, qu'il s'agisse d'un e-mail spécifique ou de nombreux e-mails correspondant à une catégorie plus large. Les messages correspondant à vos critères de recherche peuvent être téléchargés individuellement ou exportés en masse vers un compartiment S3.

Pour rechercher, télécharger ou exporter des e-mails archivés

1. Sur la page Archivage des e-mails, choisissez l'onglet Rechercher dans les archives pour afficher le tableau des archives de recherche.
2. Cliquez dans le champ Archive et choisissez une archive dans la liste suivie de Rechercher, ou affinez votre recherche en suivant les étapes ci-dessous.
3. Sélectionnez le champ Plage de dates pour élargir les options de plage de dates pour votre recherche :

   - Plage relative (par défaut) : sélectionnez le bouton radio correspondant au nombre de jours souhaité, ou choisissez une plage personnalisée en sélectionnant une unité de temps et une plage de dates allant jusqu'à 30 jours.
   - Plage absolue — Entrez une date de début et une date de fin (et une heure si vous le souhaitez) jusqu'à 30 jours.

> **Note**
>
> - La recherche dans une archive est limitée à 30 jours à la fois. Par exemple, si vous souhaitez rechercher des messages entre le 1er juin et le 31 juillet, vous devez le diviser en trois recherches comme suit :
>
>   1. 30 jours en juin.
>   2. Les 30 premiers jours de juillet.
>   3. Le 31 juillet.
>
> - Pour les dates relatives, le dernier jour se termine à minuit. Par exemple, si vous choisissez Last 7 days (7 derniers jours), le septième jour sera hier et se terminera à minuit.

4. (Facultatif) Sélectionnez le champ Filtres pour choisir parmi les filtres suivants : De, À, CC, ligne d'objet et Contient des pièces jointes. Les propriétés suivantes s'appliquent :

   - Vous pouvez créer jusqu'à 10 filtres.
   - Un filtre peut être modifié en cliquant dessus ou supprimé en sélectionnant le X.

5. Choisissez Rechercher et l'e-mail archivé correspondant à vos critères de recherche sera renseigné dans le tableau des résultats de recherche.

   - La colonne ID du message est masquée par défaut, mais elle peut être affichée en sélectionnant l'icône représentant une roue dentée pour personnaliser l'affichage du tableau.
   - Chaque recherche que vous exécutez est automatiquement enregistrée avec un identifiant de recherche unique et sera répertoriée dans le tableau de l'historique des recherches.

6. Pour afficher le texte d'un message ainsi que son enveloppe et ses informations d'en-tête, sélectionnez le bouton radio du message, puis Afficher les détails pour ouvrir la barre latérale des détails du message.

7. Pour créer un fichier local du message, sélectionnez le bouton radio du message, puis cliquez sur Télécharger le message.

8. Votre recherche filtrée peut être enregistrée dans un compartiment Amazon S3 en sélectionnant Exporter vers S3.

   a. Si vous connaissez l'URI du compartiment S3 que vous souhaitez utiliser, saisissez-le dans le champ URI S3 ; sinon, choisissez Browse S3 et sélectionnez un compartiment et un dossier S3 à utiliser sur la page S3.

   b. (Facultatif) Vous pouvez chiffrer vos messages exportés soit en saisissant votre propre AWS KMS clé dans le champ ARN de la clé KMS, soit en sélectionnant Créer une nouvelle clé. Dans le cas contraire, le chiffrement sera défini selon la méthode utilisée sur le compartiment S3 de destination (même si aucune méthode n'est utilisée).

   c. Choisissez Exporter et tous les messages trouvés dans votre recherche filtrée seront enregistrés sous forme de fichiers individuels dans le dossier S3 que vous avez sélectionné.

> **Note**
>
> Bien qu'il n'y ait aucune limite quant au nombre de messages que votre archive peut contenir, les résultats de recherche sont limités à 1 000 lignes dans le tableau des résultats de recherche.

Search history

Un historique de vos recherches est répertorié dans ce tableau afin que vous puissiez restaurer le jeu de résultats ou accéder à des ensembles de filtres complexes créés précédemment. Vous pouvez également créer de nouvelles recherches basées sur la recherche initiale en modifiant les filtres et les dates. Toutes les nouvelles recherches sont automatiquement enregistrées avec un identifiant de recherche unique et seront répertoriées dans ce tableau.

Pour consulter et utiliser vos recherches précédentes

1. Sur la page Archivage des e-mails, choisissez l'onglet Historique des recherches pour afficher le tableau Historique des recherches qui répertorie l'historique de toutes vos recherches d'e-mails archivés, la plus récente en haut. Ce tableau charge les données la première fois que vous le consultez. Si vous changez d'onglet et revenez, utilisez l'icône d'actualisation pour récupérer les données les plus récentes.
2. Cliquez dans le champ Archive et choisissez une archive dans la liste. Toutes les recherches appartenant à cette archive seront renseignées dans le tableau. Vous pouvez consulter les recherches individuelles et en faire plus en suivant les étapes ci-dessous.
3. Sélectionnez le bouton radio d'une recherche précédente, puis Afficher les résultats de recherche pour rétablir les résultats de recherche d'origine. La page d'archive de recherche s'ouvre et affiche le jeu de filtres et la plage de dates utilisés pour la recherche d'origine, ainsi que tous les messages précédemment trouvés en fonction de ces critères. Vous pouvez développer la recherche initiale de différentes manières :

   - Créez une nouvelle recherche en modifiant la plage de dates et les filtres, puis en sélectionnant Rechercher.
   - Toutes les nouvelles recherches que vous effectuez sont automatiquement enregistrées avec un identifiant de recherche unique et seront répertoriées dans le tableau de l'historique des recherches.

Export history

L'historique de vos exportations est répertorié dans ce tableau, ce qui permet d'accéder facilement au contenu du dossier d'exportation dans la console S3.

Pour consulter vos exportations récentes

1. Sur la page Archivage des e-mails, choisissez l'onglet Historique des exportations pour afficher le tableau Historique des exportations qui répertorie toutes les recherches par e-mail archivées que vous avez exportées vers un compartiment S3 au cours des 30 derniers jours. Ce tableau charge les données la première fois que vous le consultez. Si vous changez d'onglet et revenez, utilisez l'icône d'actualisation pour récupérer les données les plus récentes.
2. Si le statut d'une exportation est En file d'attente, Prétraitement ou Traitement, vous pouvez l'annuler en choisissant Annuler.
3. Sélectionnez un URI S3 pour ouvrir le dossier de compartiment de l'exportation dans la console S3 où vous pouvez voir les fichiers qu'il contient.

Manage archives

Ce tableau répertorie vos archives dans lesquelles vous avez la possibilité de créer une nouvelle archive, de rechercher une archive particulière et d'afficher ses détails, de modifier une archive ou de supprimer une archive.

Pour créer et gérer des archives

1. Sur la page Archivage des e-mails, choisissez l'onglet Gérer les archives pour afficher le tableau des archives qui répertorie toutes vos archives d'e-mails. Ce tableau charge les données la première fois que vous le consultez. Si vous changez d'onglet et revenez, utilisez l'icône d'actualisation pour récupérer les données les plus récentes.
2. Pour rechercher une archive en particulier, commencez à taper dans le champ Archives.
3. Pour afficher les détails d'une archive, sélectionnez son nom dans la colonne Nom de l'archive.
4. Pour créer une archive, sélectionnez Créer une archive.
    a. Entrez un nom unique dans le champ Nom de l'archive.
    b. (Facultatif) Sélectionnez une période de conservation dans le champ Période de conservation pour remplacer la période de conservation par défaut de 180 jours.

c. (Facultatif) Vous pouvez chiffrer votre archive soit en saisissant votre propre AWS KMS clé dans le champ ARN de la clé KMS, soit en sélectionnant Créer une nouvelle clé.

Choisissez Créer une archive.

5. Pour modifier une archive, sélectionnez son bouton radio puis Modifier.

   a. Modifiez ou modifiez le nom dans le champ Nom de l'archive.

   b. Modifiez la période de conservation dans le champ Période de conservation.

   Choisissez Mettre à jour l'archive.

6. Pour supprimer une archive, sélectionnez le bouton radio correspondant, puis cliquez sur Supprimer.

   - Tapez `delete` dans le champ Confirmer suivi de Supprimer.

     L'état de l'archive passera à En attente de suppression dans le tableau Archives et sera automatiquement supprimé au bout de 30 jours.

> **Note**
>
> Si vous souhaitez annuler cette suppression, créez un ticket pour Amazon SES dans les 30 jours.

Compléments par e-mail

Email Add Ons est un ensemble d'outils de sécurité spécialisés fournis par des fournisseurs approuvés par SES qui peuvent être utilisés pour gérer le type d'e-mail que vous autorisez à accéder à votre point de terminaison d'entrée et pour déterminer les mesures à prendre pour certains types d'e-mails. Ces outils sont des solutions certifiées de renseignement de sécurité et d'application de la loi qui sont prêtes à être intégrées à votre flux de travail de messagerie et peuvent être activées directement depuis la console Mail Manager.

Ces modules complémentaires offrent la flexibilité de choisir parmi des solutions de sécurité du courrier électronique approuvées adaptées à vos cas d'utilisation individuels et pouvant être utilisées sur la base d'un prix mesuré, au lieu d'acheter une solution unique de grande envergure qui n'est

peut-être optimisée pour aucun de vos besoins. Email Add Ons étend ses principales fonctionnalités de renseignement sur les menaces et d'application de la sécurité en fonction de la charge de travail, de sorte qu'il n'y a aucune idée de la capacité requise. Ces avantages vous permettent de garder une longueur d'avance sur les problèmes de sécurité des e-mails et de maintenir des normes de service élevées pour votre organisation.

Vous pouvez en savoir plus sur chaque module complémentaire directement sur la page des modules complémentaires par e-mail située dans la console Mail Manager, où vous aurez accès aux descriptions des produits, aux principaux avantages et aux informations sur les prix. Une fois que vous avez choisi un module complémentaire que vous souhaitez utiliser, il vous suffit de vous y abonner depuis la console Mail Manager. Une fois inscrit, vous pourrez le sélectionner comme condition de politique de trafic pour déterminer les e-mails autorisés à accéder à un point de terminaison d'entrée, ou comme condition définie de règles pour déterminer les actions à entreprendre sur des e-mails spécifiques. Le support principal pour tous les modules complémentaires est fourni par la console Mail Manager AWS et est également accessible à partir de celle-ci.

La procédure décrite dans la section suivante vous expliquera comment vous abonner à un module complémentaire de messagerie dans la console Mail Manager.

Abonnement à des modules complémentaires de messagerie dans la console Mail Manager

La procédure suivante explique comment utiliser la page Email Adds Ons de la console Mail Manager pour vous abonner à un module complémentaire afin qu'il puisse être utilisé dans n'importe lequel de vos politiques de trafic ou ensembles de règles.

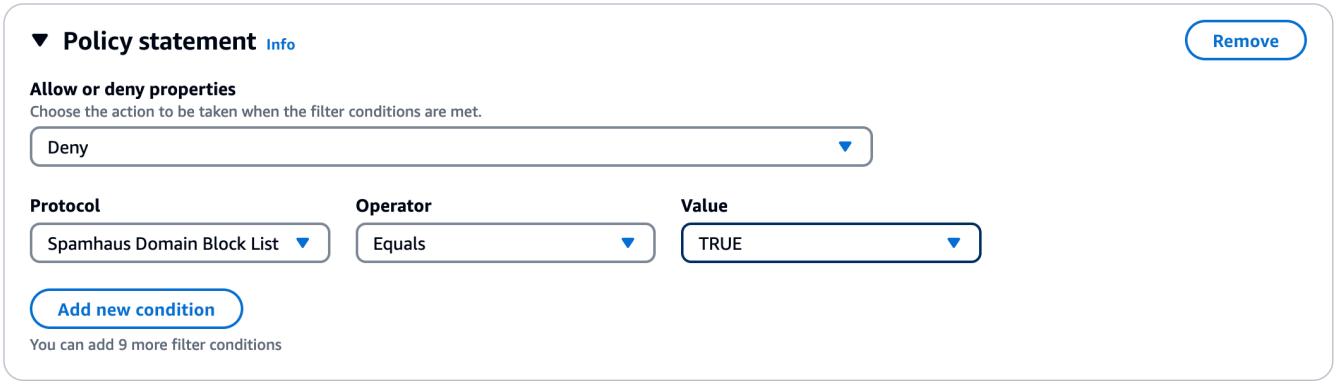
Pour s'abonner à un module complémentaire de courrier électronique à l'aide de la console

1. Connectez-vous à la console Amazon SES AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation de gauche, choisissez Email Adds Ons sous Mail Manager.
3. Sur la page des modules complémentaires par e-mail, sélectionnez le titre de n'importe quelle carte complémentaire pour ouvrir sa page d'aperçu, où vous pourrez en savoir plus sur son fonctionnement, ses principaux avantages et les informations tarifaires. Si vous souhaitez utiliser ce module complémentaire, choisissez S'abonner.

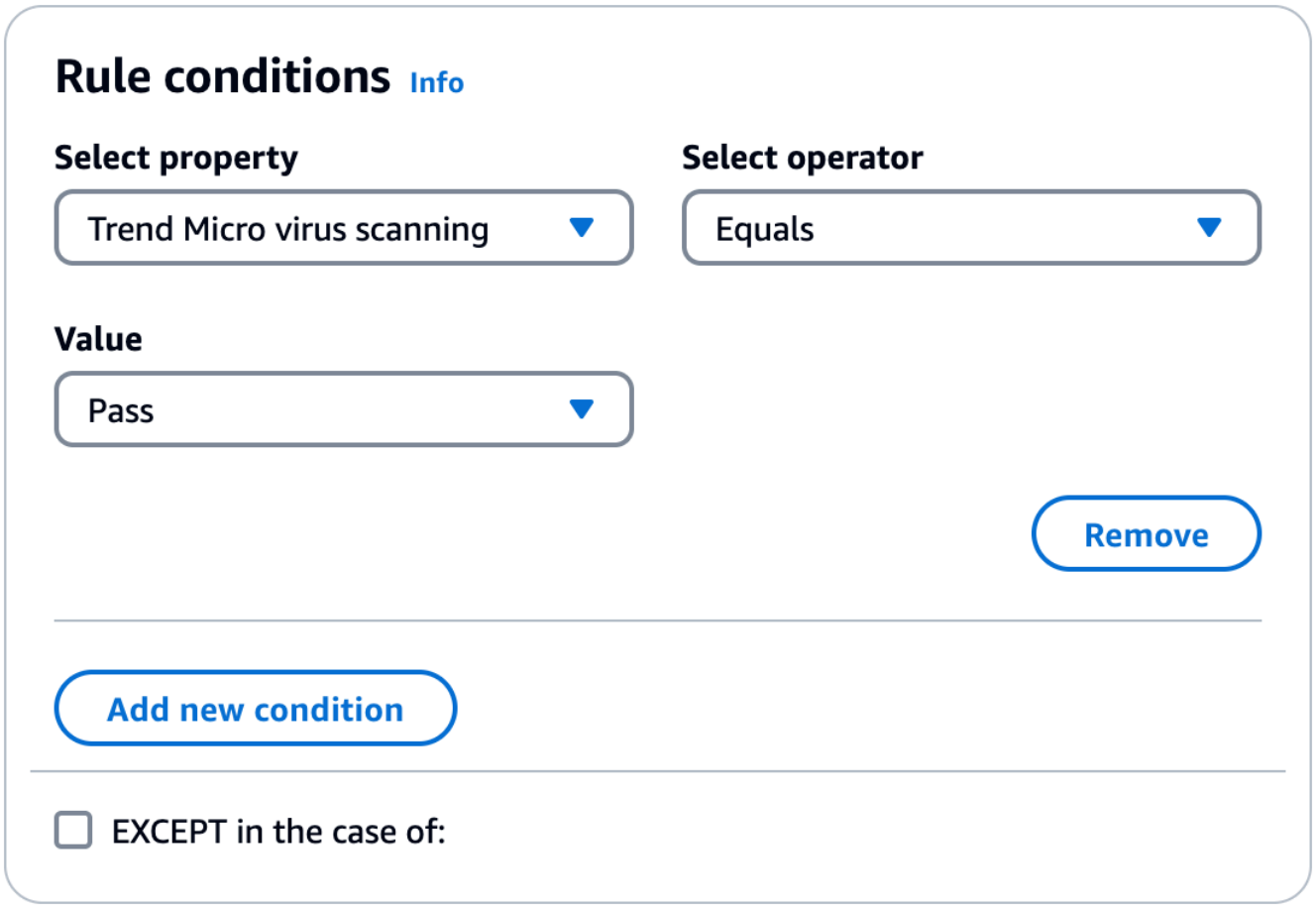
    - Lisez les termes et conditions présentés et cochez la case « J'accepte », puis « S'abonner ».

4. Une fois que vous serez abonné à un module complémentaire, vous pourrez l'intégrer à votre flux de travail de messagerie en le sélectionnant comme condition de politique de trafic pour refuser ou autoriser le courrier électronique à accéder à votre point de terminaison d'entrée, ou comme condition définie de règles pour déterminer une action à effectuer sur les messages éligibles. Les exemples suivants illustrent l'utilisation d'un module complémentaire dans une condition de déclaration de politique et dans une condition de règle :

   - En utilisant l'extension Spamhaus Domain Block List dans le cadre d'une déclaration de politique générale pour bloquer les e-mails provenant d'un domaine répertorié dans Spamhaus qui entrent dans votre terminal d'entrée :



   - Pour plus de détails sur la façon de créer des politiques de trafic et de créer des conditions de déclaration de politique à l'aide des modules complémentaires d'e-mail, consultezthe section called “Création de politiques de trafic et de déclarations de politique (console)”.
   - Utilisation du module complémentaire d'analyse antivirus Trend Micro dans une condition de règle pour déterminer une action de règle pour les e-mails qui réussissent le scan antivirus :



- Pour plus de détails sur la façon de créer des ensembles de règles et de créer des conditions de règles avec Email Add Ons, consultezthe section called “Création d'ensembles de règles et de règles (console)”.

5. Pour consulter les informations générales ou accéder à l'assistance d'un module complémentaire auquel vous êtes abonné, sélectionnez son nom sur la page des modules complémentaires par e-mail pour ouvrir sa page de présentation :

   - Dans Informations générales, vous pouvez consulter la date à laquelle vous vous êtes abonné et le nom de ressource Amazon (ARN) de votre extension.
   - Sélectionnez l'onglet Support pour accéder aux liens vers AWS Support.

6. Pour vous désabonner d'un module complémentaire :

   a. Vous devez d'abord le supprimer de toutes vos politiques de trafic ou de tous vos ensembles de règles lorsqu'il est défini dans une condition ; sinon, les étapes de désabonnement suivantes échoueront.

b. Sélectionnez son nom sur la page Email Adds Ons pour ouvrir sa page d'aperçu, puis désabonnez-vous.

c. Tapez `confirm` dans le champ Confirmer suivi de Se désabonner.

Politiques d'autorisation pour Mail Manager

Les politiques décrites dans ce chapitre constituent un point de référence unique pour les politiques nécessaires à l'utilisation des différentes fonctionnalités de Mail Manager.

Dans les pages de fonctionnalités du gestionnaire de courrier, des liens sont fournis qui vous redirigeront vers la section correspondante de cette page qui contient les politiques dont vous avez besoin pour utiliser cette fonctionnalité. Sélectionnez l'icône de copie de la politique dont vous avez besoin et collez-la comme indiqué dans le descriptif de la fonctionnalité correspondante.

Les politiques suivantes vous autorisent à utiliser les différentes fonctionnalités d'Amazon SES Mail Manager par le biais de politiques et AWS Secrets Manager de politiques d'autorisation des ressources. Si les politiques d'autorisation ne vous sont pas familières, consultez the section called “Structure de la stratégie” et Politiques d'autorisations pour AWS Secrets Manager.

Politiques d'autorisation pour le point de terminaison Ingress

Les deux politiques de cette section sont requises pour créer un point de terminaison d'entrée. Pour savoir comment créer un point de terminaison d'entrée et où utiliser ces politiques, consultezthe section called “Création d'un point de terminaison d'entrée (console)”.

Secrets Manager secrète la politique d'autorisation des ressources pour le point de terminaison d'entrée

La politique d'autorisation des ressources secrètes de Secrets Manager suivante est requise pour permettre à SES d'accéder au secret à l'aide de la ressource du point de terminaison d'entrée.

```
{
    "Version": "2012-10-17",
    "Id": "Id",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
```

```
                "Service": "ses.amazonaws.com"
            },
            "Action": "secretsmanager:GetSecretValue",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "000000000000"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ses:us-east-1:000000000000:mailmanager-
ingress-point/*"
                }
            }
        }
    ]
}
```

Politique de clé gérée par le client (CMK) KMS pour le point de terminaison d'entrée

La politique de clé gérée par le client (CMK) KMS suivante est requise pour permettre à SES d'utiliser votre clé tout en utilisant votre secret.

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "ses.amazonaws.com"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
           "kms:ViaService": "secretsmanager.us-east-1.amazonaws.com",
            "aws:SourceAccount": "000000000000"
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:ses:us-east-1:000000000000:mailmanager-ingress-
point/*"
        }
    }
}
```

Politiques d'autorisation pour le relais SMTP

Les deux politiques de cette section sont requises pour créer un relais SMTP. Pour savoir comment créer un relais SMTP et où utiliser ces politiques, consultezthe section called “Création d'un relais SMTP (console)”.

Secrets Manager secrète la politique d'autorisation des ressources pour le relais SMTP

La politique d'autorisation des ressources secrètes de Secrets Manager suivante est requise pour permettre à SES d'accéder au secret à l'aide de la ressource de relais SMTP.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Principal": {
                "Service": [
                    "ses.amazonaws.com"
                ]
            },
            "Resource": "*",
            "Condition": {
               "StringEquals": {
                   "aws:SourceAccount": "888888888888"
                },
               "ArnLike": {
                   "aws:SourceArn": "arn:aws:ses:us-east-1:888888888888:mailmanager-
smtp-relay/*"
               }
           }
        }
    ]
}
```

Politique de clé gérée par le client (CMK) KMS pour le relais SMTP

La politique de clé gérée par le client (CMK) KMS suivante est requise pour permettre à SES d'utiliser votre clé tout en utilisant votre secret.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "secretsmanager.us-east-1.amazonaws.com",
                    "aws:SourceAccount": "000000000000"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ses:us-east-1:000000000000:mailmanager-
smtp-relay/*"
                }
            }
        }
    ]
}
```

Politiques d'autorisation pour l'archivage des e-mails

Politiques d'identité IAM d'archivage de base

Il s'agit des politiques d'identité IAM permettant d'autoriser les opérations d'archivage. Ces politiques à elles seules peuvent ne pas être suffisantes pour certaines opérations (voir Archivage du chiffrement au repos avec KMS CMK et Archivage et exportation).

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ses:CreateArchive",
                "ses:TagResource"
            ],
            "Resource": [
                "arn:aws:ses:us-east-1:000000000000:mailmanager-archive/*"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:RequestTag/key-name": [
                        "value1",
                        "value2"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ses:ListArchives"
            ],
            "Resource": [
                "arn:aws:ses:us-east-1:000000000000:mailmanager-archive/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ses:GetArchive",
                "ses:DeleteArchive",
                "ses:UpdateArchive"
            ],
            "Resource": [
                "arn:aws:ses:us-east-1:000000000000:mailmanager-archive/MyArchiveID"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ses:ListArchiveSearches"
            ],
```

```
            "Resource": [
                "arn:aws:ses:us-east-1:000000000000:mailmanager-archive/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ses:GetArchiveSearch",
                "ses:GetArchiveSearchResults",
                "ses:StartArchiveSearch",
                "ses:StopArchiveSearch"
            ],
            "Resource": [
                "arn:aws:ses:us-east-1:000000000000:mailmanager-archive/MyArchiveID"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ses:GetArchiveMessage",
                "ses:GetArchiveMessageContent"
            ],
            "Resource": [
                "arn:aws:ses:us-east-1:000000000000:mailmanager-archive/MyArchiveID"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ses:ListArchiveExports"
            ],
            "Resource": [
                "arn:aws:ses:us-east-1:000000000000:mailmanager-archive/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ses:GetArchiveExport",
                "ses:StartArchiveExport",
                "ses:StopArchiveExport"
            ],
            "Resource": [
                "arn:aws:ses:us-east-1:000000000000:mailmanager-archive/MyArchiveID"
```

```
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ses:ListTagsForResource",
                "ses:UntagResource"
            ],
            "Resource": [
                "arn:aws:ses:us-east-1:000000000000:mailmanager-archive/MyArchiveID"
            ]
        }
    ]
}
```

Exportation d'archivage

Il s'agit des politiques d'identité IAM (en plus des politiques d'archivage de base ci-dessus) requises pour. `StartArchiveExport`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::MyDestinationBucketName"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectTagging",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::MyDestinationBucketName/*"
        }
    ]
}
```

Il s'agit de la politique applicable au compartiment de destination.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::MyDestinationBucketName"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectTagging",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::MyDestinationBucketName/*"
        }
    ]
}
```

> **Note**
>
> L'archivage ne prend pas en charge les clés de condition secondaires confuses (aws : SourceArnSourceAccount, aws :, aws : SourceOrg ID ou aws :SourceOrgPaths). Cela est dû au fait que l'archivage des e-mails par Mail Manager permet d'éviter le problème de confusion des adjoints en testant si l'identité appelante possède des autorisations d'écriture sur le compartiment de destination de l'exportation à l'aide de sessions d'accès direct avant de démarrer l'exportation proprement dite.

Chiffrement d'archivage au repos avec KMS CMK

Il s'agit du chiffrement basé sur les politiques KMS Customer Managed Keys (CMK) (en plus des politiques d'archivage de base ci-dessus) requises pour créer et utiliser des archives (en appelant n'importe quelle API d'archivage).

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "kms:DescribeKey",
            "kms:Decrypt",
            "kms:GenerateDataKey"
        ],
        "Resource": "arn:aws:kms:us-west-2:111122223333:key/MyKmsKeyArnID"
    }
}
```

Il s'agit de la politique de clé KMS requise pour l'archivage des e-mails.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/MyUserRoleOrGroupName"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": [
                        "ses.us-east-1.amazonaws.com"
                    ]
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

Politiques d'autorisation et de confiance pour exécuter les actions liées aux règles

Le rôle d'exécution des règles SES est un rôle AWS Identity and Access Management (IAM) qui accorde à l'exécution des règles l'autorisation d'accéder aux AWS services et aux ressources. Avant de créer une règle dans un ensemble de règles, vous devez créer un rôle IAM avec une politique qui autorise l'accès aux AWS ressources requises. SES assume ce rôle lors de l'exécution d'une action de règle. Par exemple, vous pouvez créer un rôle d'exécution de règles autorisé à écrire un message électronique dans un compartiment S3 en tant qu'action de règle à effectuer lorsque les conditions de votre règle sont remplies.

Ainsi, la politique de confiance suivante est requise en plus des politiques d'autorisation individuelles décrites dans cette section, requises pour exécuter les actions de règle Écrire dans S3, Livrer dans une boîte aux lettres et Envoyer sur Internet.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
          "Service": "ses.amazonaws.com"
        },
        "Action": "sts:AssumeRole",
        "Condition": {
          "StringEquals": {
```

```
                    "aws:SourceAccount": "888888888888"
          },
          "ArnLike": {
             "aws:SourceArn": "arn:aws:ses:us-east-1:888888888888:mailmanager-rule-set/
*"
          }
        }
      }
    ]
  }
```

Politique d'autorisation pour l'action de la règle Write to S3

La politique suivante est requise pour utiliser l'action de règle Write to S3 qui envoie le courrier électronique reçu à un compartiment S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::MyDestinationBucketName/*"
      }
    ]
  }
```

Politique d'autorisation pour l'action relative à la règle de livraison dans une boîte aux lettres

La politique suivante est requise pour utiliser l'action de règle Envoyer à la boîte aux lettres qui envoie l'e-mail reçu à un WorkMail compte Amazon.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": ["workmail:DeliverToMailbox"],
        "Resource": "arn:aws:workmail:us-
east-1:888888888888:organization/MyWorkMailOrganizationID>"
      }
```

```
    ]
  }
```

Politique d'autorisation pour l'action des règles d'envoi vers Internet

La politique suivante est requise pour utiliser l'action de règle Envoyer vers Internet qui envoie l'e-mail reçu à un domaine externe.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": ["ses:SendEmail", "ses:SendRawEmail"],
        "Resource": "arn:aws:ses:us-east-1:888888888888:identity/example.com"
      }
    ]
  }
```

Gestion des listes et des abonnements dans Amazon Simple Email Service

Vous pouvez gérer vos propres listes pour le publipostage et les abonnements, ainsi que pour la suppression des e-mails dans Amazon SES. Pour vous aider à maintenir votre réputation d'expéditeur, SES propose une suppression au niveau du compte et du jeu de configurations qui vous empêchent d'envoyer à des destinataires non valides et de nuire à votre réputation d'expéditeur. Comme mesure supplémentaire contre les e-mails de retour à l'expéditeur et les réclamations, SES peut ajouter automatiquement des liens de désabonnement à tous les e-mails sortants par le biais de la gestion des abonnements.

Chacun de ces types de listes est abordé en détail dans les sections répertoriées dans ce chapitre. Cependant, un aperçu des listes de suppression est présenté ici, car il en existe trois types de même qu'un changement clé avec la gestion globale des listes de suppression. Il est suggéré de lire cette présentation avant de travailler avec l'une des listes abordées dans ce chapitre.

Présentation des trois types de listes de suppression

La fonction de suppression de la liste de suppression globale n'est plus destinée aux clients et vous n'interagissez plus avec elle pour gérer les listes de suppression. La liste de suppression globale fonctionne et est gérée en arrière-plan par SES. En tant que client, vous disposez désormais de listes de suppression au niveau du compte et du jeu de configurations qui vous offrent un contrôle plus personnalisé sur la façon dont vous gérez la suppression des e-mails pour votre propre compte.

Les différents types de listes de suppression, leur portée et les avantages qu'elles offrent sont expliqués ci-dessous. Les trois types de listes de suppression utilisés dans Amazon SES sont les suivants :

- Liste de suppression globale – détenue et gérée par SES pour protéger la réputation des adresses dans le pool d'adresses IP partagées de SES.
- Account-level suppression list (Liste de suppression au niveau du compte) : détenue et gérée par le client pour protéger la réputation de son compte ; elle supplante la liste de suppression globale.
- Suppression au niveau du jeu de configurations – possédé et géré par le client pour fournir un contrôle conditionnel ou précis sur la gestion des listes de suppression ;elle supplante la liste de suppression au niveau du compte.

La liste de suppression globale était le seul type de liste de suppression jusqu'à ce que la suppression au niveau du compte et du jeu de configurations ait été introduite dans la nouvelle console Amazon SES et l'API v2. La liste de suppression globale est détenue et gérée par SES pour protéger la réputation de SES. Cette mesure est nécessaire, car tous les clients SES partagent le même groupe d'adresses IP (à moins qu'ils ne disposent d'adresses IP dédiées), il donc est important pour SES de s'assurer que les clients n'envoient pas de spam ou tout ce qui pourrait avoir un impact négatif sur la réputation de ces adresses IP dans le groupe d'IP partagé de SES. Bien que vous n'ayez plus d'interaction directe avec la liste de suppression globale, elle fonctionne toujours en arrière-plan et les principes généraux du fonctionnement de la liste de suppression globale peuvent également être appliqués pour expliquer ceux du fonctionnement des autres types de listes de suppression. Consultez Liste de suppression globale Amazon SES.

> **Note**
>
> Le formulaire de demande de suppression de la liste de suppression globale ne se trouve plus dans la console Amazon SES, car la liste de suppression au niveau du compte l'a remplacée pour tous les avantages expliqués dans cette section.

La liste de suppression au niveau du compte a été introduite afin que les clients puissent créer et contrôler leurs propres listes de suppression et leur réputation. Ainsi, la liste de suppression au niveau du compte s'applique uniquement à votre compte. L'interface de liste de suppression au niveau du compte de la nouvelle console permet de gérer facilement les adresses de votre liste de suppression au niveau du compte, y compris des actions en bloc pour ajouter ou supprimer des adresses. Si une adresse figure sur la liste de suppression globale, mais pas sur la liste de suppression au niveau de votre compte (ce qui signifie que vous souhaitez pouvoir y envoyer des messages), et que vous y envoyez effectivement des messages, Amazon SES tentera toujours de livrer, mais en cas de retour à l'expéditeur, celui-ci n'affectera que votre propre réputation, et personne d'autre ne sera affecté par les rebonds puisque les destinataires ne peuvent pas envoyer de messages à cette adresse e-mail s'ils n'utilisent pas leur propre liste de suppression au niveau du compte ; autrement dit, la liste de suppression au niveau du compte prévaut sur la liste de suppression globale pour votre compte uniquement. Consultez Utilisation de la liste de suppression au niveau du compte Amazon SES.

Lasuppression au niveau du jeu de configurations vous permet de configurer des personnalisations de suppression et des dérogations à la suppression au niveau du compte, mais aussi d'utiliser plusieurs jeux de configurations spécifiquement créés pour différents scénarios d'envoi d'e-mails. Par exemple, si votre liste de suppression au niveau du compte est configurée pour ajouter des adresses

de retour à l'expéditeur et de réclamation, mais que vous disposez d'une démographie spécifique de messagerie définie dans un ensemble de configuration pour lequel vous êtes uniquement intéressé par l'ajout d'adresses de réclamation, vous pouvez y parvenir en activant cette option. La suppression du jeu de configurations remplace la suppression de sorte que les adresses e-mail soient ajoutées à votre liste de suppression au niveau de votre compte uniquement pour les plaintes (pas les retours à l'expéditeur et les plaintes tels que définis dans la liste de suppression au niveau de votre compte) à partir des e-mails envoyés avec ce jeu de configurations. Avec la suppression au niveau du jeu de configurations, il existe différents niveaux de suppression au niveau du compte, y compris la possibilité de ne pas utiliser de suppression du tout. Consultez Utilisation de la suppression au niveau du jeu de configurations pour remplacer votre liste de suppression au niveau du compte.

Liste de suppression globale Amazon SES

Amazon SES gère et exploite en arrière-plan une liste de suppression globale interne. Lorsqu'un client SES envoie un e-mail qui entraîne un retour à l'expéditeur, SES ajoute l'adresse e-mail qui a généré le retour à l'expéditeur à une liste de suppression globale. La liste de suppression globale est globale dans le sens où elle s'applique à tous les clients SES. En d'autres termes, si un autre client tente d'envoyer un e-mail à une adresse figurant sur la liste de suppression globale, SES accepte le message, mais ne l'envoie pas, car l'adresse e-mail est supprimée.

La fonction de demande de suppression d'adresse e-mail de la liste de suppression globale n'est plus destinée au client et vous n'interagissez plus avec elle pour gérer les listes de suppression. Pour remplacer cette fonctionnalité, Amazon SES propose désormais une nouvelle façon de gérer vos listes de suppression en proposant des listes de suppression au niveau du compte et des listes de suppression au niveau du jeu de configurations. Ces listes offrent un contrôle plus personnalisé sur la votre gestion de la suppression des e-mails pour votre compte. Pour de plus amples informations, veuillez consulter Utilisation de la liste de suppression au niveau du compte Amazon SES et Utilisation de la suppression au niveau du jeu de configurations pour remplacer votre liste de suppression au niveau du compte.

> **Important**
>
> Le formulaire de demande de suppression d'adresse e-mail de la liste de suppression globale n'est plus dans la console Amazon SES, car la liste de suppression au niveau du compte l'a supplanté. Pour savoir comment utiliser la liste de suppression au niveau du compte, consultez Utilisation de la liste de suppression au niveau du compte Amazon SES.

Considérations relatives à la liste de suppression globale

Facteurs clés concernant la liste de suppression globale :

- SES exploite et gère la liste de suppression globale en arrière-plan. Il vous est impossible d'interagir directement avec elle. En revanche, vous pouvez la remplacer en utilisant votre liste de suppression au niveau du compte.
- La liste de suppression globale est activée par défaut pour tous les comptes SES. Vous ne pouvez pas la désactiver.
- Dans le mesure où SES applique la liste de suppression globale à tous les clients, vous ne pouvez pas interroger la liste de suppression globale ou y ajouter des adresses manuellement.
- Lorsqu'une adresse e-mail produit un message d'erreur définitif, SES ajoute l'adresse à la liste de suppression globale pour une courte période. Une fois cette période écoulée, SES supprime l'adresse de la liste. Si l'adresse produit un autre message d'erreur définitif, SES l'ajoute à la liste de suppression globale pour une période plus longue et la supprime à la fin de cette période. La durée pendant laquelle une adresse reste dans la liste de suppression globale augmente à chaque fois que l'adresse produit un message d'erreur définitif. Les adresses peuvent rester dans la liste de suppression globale pendant 14 jours maximum.
- Si vous tentez d'envoyer un message à une adresse de la liste de suppression globale, SES accepte le message, mais ne l'envoie pas. SES génère une notification de retour à l'expéditeur avec la valeur `bounceType` pour `Permanent` et la valeur `bounceSubType` pour `Suppressed`. La réception de ce type de notification de retour à l'expéditeur est le seul moyen de savoir si une adresse figure sur la liste de suppression globale. Vous ne pouvez pas interroger la liste de suppression globale.
- SES comptabilise les messages que vous envoyez aux adresses figurant sur la liste de suppression globale dans le taux de retour à l'expéditeur de votre compte et dans votre quota d'envoi quotidien.
- Comme pour toute adresse électronique qui génère un retour à l'expéditeur définitif, vous avez tout intérêt à retirer de votre liste de diffusion les adresses qui provoquent un retour de la liste de suppression, sauf si vous êtes certain que l'adresse est valide.
- Les retours de la liste de suppression sont comptabilisés dans votre taux de retours à l'expéditeur. Si votre taux de retour à l'expéditeur est trop élevé, votre compte peut être placé sous surveillance ou la capacité de votre compte à envoyer des e-mails peut être suspendue.

> **Note**
>
> Il est indispensable de bien comprendre les interdépendances entre les trois listes de suppression et leur hiérarchie. Pour ce faire, consultez Présentation des trois types de listes de suppression.

Utilisation de la liste de suppression au niveau du compte Amazon SES

La liste de suppression au niveau du compte Amazon SES a été introduite afin que les clients puissent créer et contrôler leurs propres listes de suppression et leur réputation. Ainsi, la liste de suppression au niveau du compte s'applique uniquement à votre compte. L'interface de liste de suppression au niveau du compte de la console SES permet de gérer facilement les adresses de votre liste de suppression au niveau de votre compte, y compris des actions en bloc pour ajouter ou supprimer des adresses.

La liste de suppression au niveau de votre compte SES s'applique à votre Compte AWS dans la Région AWS actuelle. Vous pouvez ajouter ou supprimer manuellement, individuellement ou en bloc, des adresses de votre liste de suppression au niveau de votre compte en utilisant l'API v2 ou la console SES.

> **Note**
>
> Pour ajouter ou supprimer des adresses en bloc, vous devez disposer d'un accès en production. Pour en savoir plus sur l'environnement de test (sandbox), veuillez consulter Demande d'accès à la production (sortie du sandbox d'Amazon SES).

Considérations relatives à la liste de suppression au niveau du compte Amazon SES

Vous devez tenir compte des facteurs suivants lorsque vous utilisez la liste de suppression au niveau de votre compte :

- Si vous avez commencé à utiliser Amazon SES après le 25 novembre 2019, votre compte utilise la liste de suppression au niveau du compte par défaut pour les retours à l'expéditeur et les

réclamations. Si vous avez commencé à utiliser SES avant cette date, vous devez activer cette fonction via l'opération `PutAccountSuppressionAttributes` dans l'API SES.

- Si vous tentez d'envoyer un message à une adresse de la liste de suppression au niveau du compte, dont le motif de suppression correspond au motif de suppression choisi dans vos paramètres de suppression au niveau du compte, SES accepte le message, mais ne l'envoie pas. Si les motifs ne correspondent pas, SES envoie le message. Pour clarifier ce point, consultez les exemples suivants :
  - Vous avez défini les paramètres de suppression au niveau du compte en utilisant le motif de suppression Retours à l'expéditeur uniquement. Dans ce cas, SES ne tentera pas d'envoyer le message aux adresses figurant dans la liste de suppression au niveau du compte pour lesquelles le motif de suppression est Retour à l'expéditeur.
  - Vous avez défini les paramètres de suppression au niveau du compte en utilisant le motif de suppression Retours à l'expéditeur et réclamations. Dans ce cas, SES ne tentera pas d'envoyer le message aux adresses figurant dans la liste de suppression au niveau du compte pour lesquelles le motif de suppression est Retour à l'expéditeur ou Réclamation.
  - Vous avez défini les paramètres de suppression au niveau du compte en utilisant le motif de suppression Retours à l'expéditeur uniquement. Dans ce cas, SES tentera d'envoyer le message aux adresses figurant dans la liste de suppression au niveau du compte pour lesquelles le motif de suppression est Réclamation (car dans ce cas, les motifs ne correspondent pas).
- SES ne comptabilise pas les messages que vous envoyez aux adresses de la liste de suppression au niveau de votre compte dans le taux de retour à l'expéditeur de votre compte.
- Si une adresse figure sur la liste de suppression globale, mais pas sur la liste de suppression au niveau de votre compte (ce qui signifie que vous souhaitez lui envoyer l'e-mail) et que vous envoyez l'e-mail à cette adresse, SES tente d'effectuer la livraison ; cependant, en cas de retour à l'expéditeur, il sera pris en compte dans le taux de retour de votre compte et dans votre quota d'envois quotidien.
- SES comptabilise les messages que vous envoyez aux adresses de la liste de suppression au niveau de votre compte dans votre quota d'envoi quotidien.
- Les adresses e-mail figurant sur la liste de suppression au niveau de votre compte y restent jusqu'à ce que vous les supprimiez.
- Si la capacité de votre compte à envoyer des e-mails est interrompue, SES supprime automatiquement les adresses de la liste de suppression au niveau de votre compte après 90 jours. Si la capacité de votre compte à envoyer des e-mails est rétablie avant la fin de cette période de 90 jours, les adresses de la liste ne sont pas supprimées.

- Gmail ne fournit pas de données de plainte à SES. Si un destinataire utilise le bouton Spam du client Web Gmail pour signaler un message de votre part reçu en tant que courrier indésirable, il n'est pas ajouté à la liste de suppression au niveau de votre compte.
- Vous pouvez activer la liste de suppression au niveau de votre compte si ce dernier se trouve dans l'environnement de test (sandbox) SES. Toutefois, vous ne pouvez pas utiliser l'opération PutSuppressedDestination ou CreateImportJob tant que votre compte n'est pas supprimé de l'environnement de test (sandbox). Pour en savoir plus sur l'environnement de test (sandbox), veuillez consulter Demande d'accès à la production (sortie du sandbox d'Amazon SES).
- Seuls les messages d'erreur définitifs sont ajoutés à la liste de suppression au niveau de votre compte. Pour plus d'informations sur les différences entre les messages d'erreur définitifs et temporaires, consultez the section called “Après l'envoi d'un e-mail par Amazon SES”.
- Lorsque vous utilisez la liste de suppression au niveau du compte, SES ajoute également à la liste de suppression globale les adresses qui provoquent des retours à l'expéditeur définitifs.

Activation de la liste de suppression au niveau du compte Amazon SES

Vous pouvez utiliser l'opération PutAccountSuppressionAttributes dans l'API Amazon SES v2 pour activer et configurer la liste de suppression au niveau de votre compte. Vous pouvez configurer rapidement et facilement ce paramètre en utilisant l' AWS CLI. Pour en savoir plus sur l'installation et la configuration de l'AWS CLI, consultez le Guide de l'utilisateur de l'AWS Command Line Interface.

Pour configurer la liste de suppression au niveau de votre compte à l'aide de la AWS CLI

- Sur la ligne de commande, entrez la commande suivante :

  Linux, macOS, or Unix

  ```
  aws sesv2 put-account-suppression-attributes \
  --suppressed-reasons BOUNCE COMPLAINT
  ```

  Windows

  ```
  aws sesv2 put-account-suppression-attributes `
  --suppressed-reasons BOUNCE COMPLAINT
  ```

Pour activer la liste de suppression au niveau de votre compte, vous devez indiquer au moins une raison pour le paramètre `suppressed-reasons`. Vous pouvez spécifier `BOUNCE` ou `COMPLAINT`,ou les deux, comme indiqué dans l'exemple précédent.

Pour configurer la liste de suppression au niveau de votre compte en utilisant la console SES :

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES sur la page https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Suppression list (Liste de suppression).
3. Dans Account-level settings (Paramètres au niveau du compte), choisissez Edit (Modifier).
4. Dans Suppression list (Liste de suppression), cochez la case Enabled (Activé).
5. Pour Suppression reasons (Raisons de suppression), sélectionnez l'une des raisons pour lesquelles les adresses e-mail des destinataires doivent être automatiquement ajoutées à la liste de suppression au niveau de votre compte.
6. Choisissez Enregistrer les modifications.

Activation de la liste de suppression au niveau du compte Amazon SES pour un jeu de configuration

Vous pouvez également configurer la suppression au niveau de votre compte Amazon SES de sorte qu'elle s'applique uniquement à des jeux de configurations spécifiques. Dans ce cas, les adresses ne sont ajoutées à la liste de suppression que si vous avez spécifié le jeu de configuration lorsque vous avez envoyé l'e-mail à l'origine de l'événement de retour à l'expéditeur ou de plainte.

> **Note**
>
> La procédure suivante suppose que vous avez déjà installé le AWS CLI. Pour en savoir plus sur l'installation et la configuration de l'AWS CLI, consultez le Guide de l'utilisateur de l'AWS Command Line Interface.

Pour configurer la liste de suppression au niveau de votre compte pour un jeu de configurations à l'aide de l'AWS CLI

- Sur la ligne de commande, entrez la commande suivante :

  Linux, macOS, or Unix

  ```
  aws sesv2 put-configuration-set-suppression-options \
  --configuration-set-name configSet \
  --suppressed-reasons BOUNCE COMPLAINT
  ```

  Windows

  ```
  aws sesv2 put-configuration-set-suppression-options `
  --configuration-set-name configSet `
  --suppressed-reasons BOUNCE COMPLAINT
  ```

  Dans l'exemple précédent, remplacez *ConfigSet* par le nom du jeu de configurations devant utiliser la liste de suppression au niveau de votre compte.

Pour configurer la liste de suppression au niveau de votre compte pour un jeu de configurations en utilisant la console SES :

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Configuration sets (Jeux de configurations).
3. Dans Jeux de configurations, choisissez le nom du jeu de configurations que vous souhaitez configurer avec une suppression personnalisée.
4. Dans Suppression list options (Options de liste de suppression), choisissez Edit (Modifier).
5. La section Suppression list options (Options de liste de suppression) fournit un ensemble de décisions permettant de définir une suppression personnalisée en commençant par l'option permettant d'utiliser ce jeu de configurations pour supplanter la suppression au niveau de votre compte. La carte logique de suppression au niveau du jeu de configurations vous aidera à comprendre les effets des combinaisons de remplacement. Ces sélections à plusieurs niveaux

de remplacement peuvent être combinées pour implémenter trois niveaux de suppression différents :

a. Use account-level suppression (Utiliser la suppression au niveau du compte) : ne remplace pas la suppression au niveau de votre compte et n'implémente aucune suppression au niveau du jeu de configurations. En fait, tout e-mail envoyé à l'aide de ce jeu de configurations utilisera simplement la suppression au niveau de votre compte. Pour cela :

   - Dans Suppression list settings (Paramètres de la liste de suppression), décochez la case Override account level settings (Remplacer les paramètres au niveau du compte).

b. Do not use any suppression (N'utiliser aucune suppression) : remplace la suppression au niveau de votre compte sans activer la suppression au niveau du jeu de configurations. Cela signifie que tout e-mail envoyé à l'aide de ce jeu de configurations n'utilisera aucune suppression au niveau de votre compte ; en d'autres termes, toute suppression est annulée. Pour cela :

   i. Dans Suppression list settings (Paramètres de la liste de suppression), cochez la case Override account level settings (Remplacer les paramètres au niveau du compte).

   ii. Dans Suppression list (Liste de suppression), décochez la case Enabled (Activé).

c. Use configuration set-level suppression (Utiliser la suppression au niveau du jeu de configurations) : remplace la suppression au niveau de votre compte par des paramètres de liste de suppression personnalisés définis dans ce jeu de configurations. Cela signifie que tout e-mail envoyé à l'aide de ce jeu de configurations utilisera uniquement ses propres paramètres de suppression et ignorera tous les paramètres de suppression au niveau du compte. Pour cela :

   i. Dans Suppression list settings (Paramètres de la liste de suppression), cochez la case Override account level settings (Remplacer les paramètres au niveau du compte).

   ii. Dans Suppression list (Liste de suppression), cochez la case Enabled (Activé).

   iii. Dans Specify the reason(s)... (Spécifiez la ou les raisons...), sélectionnez l'un des motifs de suppression à utiliser pour ce jeu de configurations.

6. Choisissez Enregistrer les modifications.

Ajout d'adresses e-mail individuelles à la liste de suppression au niveau du compte Amazon SES

Vous pouvez ajouter des adresses individuelles à la liste de suppression au niveau de votre compte Amazon SES à l'aide de l'opération PutSuppressedDestination dans l'API SES v2. Le nombre d'adresses que vous pouvez ajouter à la liste de suppression au niveau de votre compte n'est pas limité.

> **Note**
>
> La procédure suivante suppose que vous avez déjà installé le AWS CLI. Pour en savoir plus sur l'installation et la configuration de l'AWS CLI, consultez le Guide de l'utilisateur de l'AWS Command Line Interface.

Pour ajouter des adresses individuelles à la liste de suppression au niveau de votre compte à l'aide de l'AWS CLI

- Sur la ligne de commande, entrez la commande suivante :

  Linux, macOS, or Unix

  ```
  aws sesv2 put-suppressed-destination \
  --email-address recipient@example.com \
  --reason BOUNCE
  ```

  Windows

  ```
  aws sesv2 put-suppressed-destination `
  --email-address recipient@example.com `
  --reason BOUNCE
  ```

  Dans l'exemple précédent, remplacez *recipient@example.com* par l'adresse e-mail que vous souhaitez ajouter à la liste de suppression au niveau de votre compte, et *BOUNCE* par la raison pour laquelle vous ajoutez l'adresse à la liste de suppression (les valeurs acceptables sont `BOUNCE` et `COMPLAINT`).

Pour ajouter des adresses individuelles à la liste de suppression au niveau de votre compte à l'aide de la console SES :

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES sur la page https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Suppression list (Liste de suppression).
3. Dans Suppression list (Liste de suppression), choisissez Add email address (Ajout d'une adresse e-mail).
4. Saisissez une adresse e-mail dans le champ Email address (Adresse e-mail), puis sélectionnez une raison dans Suppression reason (Raison de suppression). Si vous devez saisir d'autres adresses, choisissez Enter another address (Saisir une autre adresse) et répétez l'opération pour chaque adresse supplémentaire.
5. Lorsque vous avez terminé de saisir les adresses, vérifiez la précision de vos entrées. Si vous décidez que l'une de vos entrées ne doit pas faire partie de cette soumission, cliquez sur le bouton Remove (Supprimer).
6. Choisissez Save changes (Enregistrer les modifications) pour ajouter les adresses e-mail saisies à votre liste de suppression au niveau du compte.

Ajout d'adresses e-mail en bloc à la liste de suppression au niveau de votre compte Amazon SES

Vous pouvez ajouter des adresses en bloc en chargeant d'abord votre liste de contacts dans un objet Amazon S3, puis en utilisant l'opération CreateImportJob dans l'API Amazon SES v2.

> **Note**
>
> - Le nombre d'adresses que vous pouvez ajouter à la liste de suppression au niveau de votre compte n'est pas limité, mais il existe une limite d'ajout de 100 000 d'adresses dans un objet Amazon S3 par appel d'API.
> - Si votre source de données est un compartiment S3, celui-ci doit se trouver dans la région où vous effectuez l'importation.

Pour ajouter des adresses e-mail en bloc à votre liste de suppression au niveau du compte, procédez comme suit.

- Téléchargez votre liste d'adresses dans un objet Amazon S3 au format CSV ou JSON.

  Exemple de format CSV pour ajouter des adresses :

  recipient1@example.com,*BOUNCE*

  recipient2@example.com,*COMPLAINT*

  Seuls les nouveaux fichiers JSON délimités par une ligne sont pris en charge. Dans ce cas, chaque ligne est un objet JSON complet qui contient une définition d'adresse distincte.

  Exemple de format JSON pour ajouter des adresses :

  {"emailAddress":"*recipient1@example.com*","reason":"*BOUNCE*"}

  {"emailAddress":"*recipient2@example.com*","reason":"*COMPLAINT*"}

  Dans les exemples précédents, remplacez *recipient1@example.com* et *recipient2@example.com* par l'adresse e-mail que vous souhaitez ajouter à la liste de suppression au niveau de votre compte. Les raisons acceptables pour lesquelles vous ajoutez les adresses à la liste de suppression sont *BOUNCE* et *COMPLAINT*.
- Autoriser SES à lire l'objet Amazon S3.

  Appliquée à un compartiment Amazon S3, la politique suivante accorde à SES l'autorisation de lire ce compartiment. Pour plus d'informations sur l'attachement de stratégies de compartiment vers Amazon S3, veuillez consulter Stratégies de compartiment et stratégies d'utilisateur dans le Guide de l'utilisateur d'Amazon Simple Storage Service.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSESGet",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": "s3:GetObject",
```

```
            "Resource": "arn:aws:s3:::BUCKET-NAME/OBJECT-NAME",
            "Condition": {
                "StringEquals": {
                    "aws:Referer": "AWSACCOUNTID"
                }
            }
        }
    ]
}
```

- Autoriser SES à utiliser votre clé AWS KMS.

  Si l'objet Amazon S3 est chiffré avec une clé AWS KMS, vous devez attribuer à Amazon SES l'autorisation d'utiliser la clé AWS KMS. SES ne peut obtenir l'autorisation qu'à partir d'une clé gérée par le client, et non d'une clé KMS par défaut. Vous devez accorder à SES l'autorisation d'utiliser la clé gérée par le client en ajoutant une instruction à la politique de la clé.

  Collez l'instruction de politique suivante dans la politique de clé pour permettre à SES d'utiliser votre clé gérée par le client.

```
{
   "Sid": "AllowSESToDecrypt",
   "Effect": "Allow",
   "Principal": {
       "Service":"ses.amazonaws.com"
   },
   "Action": [
       "kms:Decrypt",
   ],
   "Resource": "*"
}
```

- Utilisez l'opération CreateImportJob dans l'API SES v2.

> **Note**
>
> L'exemple suivant suppose que vous avez déjà installé le AWS CLI. Pour en savoir plus sur l'installation et la configuration de l'AWS CLI, consultez le Guide de l'utilisateur de l'AWS Command Line Interface.

En ligne de commande, entrez la commande suivante. Remplacez *s3bucket* par le nom d'un compartiment Amazon S3 et *s3object* par le nom d'un objet Amazon S3.

```
aws sesv2 create-import-job --import-destination
 SuppressionListDestination={SuppressionListImportAction=PUT} --import-data-source
 S3Url=s3://s3bucket/s3object,DataFormat=CSV
```

Pour ajouter des adresses e-mail en bloc à la liste de suppression au niveau de votre compte à l'aide de la console SES :

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES sur la page https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Suppression list (Liste de suppression).
3. Dans Suppression list (Liste de suppression), développez le bouton Bulk actions (Actions en bloc) et sélectionnez Add email addresses in bulk (Ajouter des adresses e-mail en bloc).
4. Dans Bulk action specifications (Spécifications de l'action en bloc), sélectionnez l'un des points (a) Choose file from S3 bucket (Choisir le fichier dans le compartiment S3) ou (b) Import From File (Importer le fichier depuis) – les procédures sont données pour chaque méthode d'importation :

    a. Choose file from S3 bucket (Choisir le fichier dans le compartiment S3) – si votre fichier source est déjà stocké dans un compartiment Amazon S3 :

        i. Si vous connaissez l'URI du compartiment Amazon S3 que vous souhaitez utiliser, saisissez-le dans le champ URI Amazon S3 ; sinon, choisissez Parcourir S3 :

            A. Dans Buckets (Compartiments), sélectionnez le nom du compartiment S3.

            B. Dans Objects (Objets), sélectionnez le nom du fichier, puis sélectionnez Choose (Choisir) – vous serez renvoyé à Bulk action specifications (Spécifications de l'action en bloc).

            C. (Facultatif) Si vous souhaitez être redirigé vers la console Amazon S3 pour afficher les détails de votre objet S3, choisissez View (Afficher).

        ii. Dans File format (Format de fichier), sélectionnez le format du fichier que vous avez choisi d'importer depuis votre compartiment Amazon S3.

iii. Choisissez Add email addresses (Ajout d'adresses e-mail) pour lancer l'importation d'adresses depuis votre fichier – un tableau sous l'onglet Bulk actions (Actions en bloc) s'affiche.

b. Import From File (Importer depuis un fichier) – si vous avez un fichier source local à charger vers un compartiment Amazon S3 nouveau ou existant :

i. Dans Import source file (Importer le fichier source), sélectionnez Choose file (Choisir le fichier).

ii. Sélectionnez le fichier JSON ou CSV dans le navigateur de fichiers et choisissez Open (Ouvrir) – vous verrez le nom, la taille et la date de votre fichier s'affichent sous le bouton Choose file (Choisir le fichier).

iii. Développer Amazon S3 bucket (Compartiment Amazon S3) et sélectionnez le compartiment S3.

- Pour charger votre fichier dans un nouveau compartiment, choisissez Create S3 bucket (Créer un compartiment S3), saisissez un nom dans le Bucket name (Nom du compartiment) et choisissez Create bucket (Créer un compartiment).

iv. Choisissez Add email addresses (Ajout d'adresses e-mail) pour lancer l'importation d'adresses depuis votre fichier – un tableau sous l'onglet Bulk actions (Actions en bloc) s'affiche.

5. Quelle que soit la méthode d'importation que vous avez utilisée, votre ID de tâche sera répertorié dans Bulk actions (Actions en bloc) avec le type d'importation, le statut et la date – pour afficher les détails de la tâche, sélectionnez l'ID de tâche.

6. Sélectionnez la Suppression list (Liste de suppression) et toutes les adresses e-mail importées avec succès sont affichées avec leur raison de suppression et leur date d'ajout. Les options suivantes sont disponibles :

a. Sélectionnez une adresse e-mail ou cochez la case correspondante et choisissez View report (Afficher le rapport) pour en afficher les détails. (S'il s'agit d'une adresse qui a été automatiquement ajoutée à votre liste de suppression en raison d'un retour à l'expéditeur ou d'une réclamation, des informations seront affichées sur l'événement de commentaires qui a provoqué son ajout, y compris des détails sur le message de l'e-mail qui a produit l'événement déclencheur.)

b. Cochez la case correspondante d'une ou de plusieurs adresses e-mail que vous souhaitez supprimer de la liste de suppression de votre compte, puis choisissez Remove (Supprimer).

Affichage d'une liste d'adresses figurant dans la liste de suppression au niveau de votre compte Amazon SES

Vous pouvez afficher une liste de toutes les adresses e-mail figurant dans la liste de suppression au niveau de votre compte à l'aide de l'opération ListSuppressedDestinations dans l'API SES v2.

> **Note**
>
> La procédure suivante suppose que vous avez déjà installé le AWS CLI. Pour en savoir plus sur l'installation et la configuration de l'AWS CLI, consultez le Guide de l'utilisateur de l'AWS Command Line Interface.

Pour afficher la liste de toutes les adresses de messagerie figurant dans la liste de suppression au niveau de votre compte

- Sur la ligne de commande, entrez la commande suivante :

```
aws sesv2 list-suppressed-destinations
```

La commande précédente renvoie toutes les adresses de messagerie qui se trouvent dans la liste de suppression au niveau de votre compte pour votre compte. La sortie ressemble à l'exemple suivant :

```
{
    "SuppressedDestinationSummaries": [
        {
            "EmailAddress": "recipient2@example.com",
            "Reason": "COMPLAINT",
            "LastUpdateTime": "2020-04-10T21:03:05Z"
        },
        {
            "EmailAddress": "recipient0@example.com",
            "Reason": "COMPLAINT",
            "LastUpdateTime": "2020-04-10T21:04:26Z"
        },
        {
            "EmailAddress": "recipient1@example.com",
            "Reason": "BOUNCE",
            "LastUpdateTime": "2020-04-10T22:07:59Z"
```

```
        }
    ]
}
```

- Remarque— Si votre sortie comprend un champ « NextToken » avec une valeur de chaîne, des adresses e-mail supplémentaires sont présentes dans la liste de suppression de votre compte. Pour voir les autres adresses supprimées, envoyez une autre demande à `ListSuppressedDestinations` et transmettez la valeur de chaîne renvoyée dans le paramètre `--next-token`. Ainsi :

  ```
  aws sesv2 list-suppressed-destinations --next-token string
  ```

  Dans la commande précédente, remplacez *chaîne* par la valeur NextToken renvoyée.

  Pour plus d'informations, consultez How to list over 1000 email addresses from account-level suppression list.

Vous pouvez utiliser l'option `StartDate` pour afficher uniquement les adresses e-mail ayant été ajoutées à la liste après une certaine date.

Pour afficher la liste des adresses ayant été ajoutées à la liste de suppression au niveau de votre compte après une date spécifique

- Sur la ligne de commande, entrez la commande suivante :

  ```
  aws sesv2 list-suppressed-destinations --start-date 1604394130
  ```

  Dans la commande précédente, remplacez *1604394130* par l'horodatage Unix de la date de début.

Vous pouvez également utiliser l'option `EndDate` pour afficher uniquement les adresses de messagerie ayant été ajoutées à la liste avant une certaine date.

Pour afficher la liste des adresses ayant été ajoutées à la liste de suppression au niveau de votre compte avant une date spécifique

- Sur la ligne de commande, entrez la commande suivante :

```
aws sesv2 list-suppressed-destinations --end-date 1611126000
```

Dans la commande précédente, remplacez *1611126000* par l'horodatage Unix de la date de fin.

Sur la ligne de commande Linux, macOS ou Unix, vous pouvez également lancer l'utilitaire intégré `grep` pour rechercher des adresses ou des domaines spécifiques.

Pour rechercher une adresse spécifique dans la liste de suppression au niveau de votre compte

- Sur la ligne de commande, entrez la commande suivante :

  ```
  aws sesv2 list-suppressed-destinations | grep -A2 'example.com'
  ```

  Dans la commande précédente, remplacez *example.com* par la chaîne de texte (l'adresse ou le domaine) que vous souhaitez rechercher.

Pour afficher une liste de toutes les adresses e-mail qui sont sur la liste de suppression au niveau de votre compte en utilisant la console SES :

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES sur la page https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Suppression list (Liste de suppression).
3. Dans le panneau Suppression list (Liste de suppression), toutes les adresses e-mail de la liste de suppression au niveau de votre compte sont affichées avec leur raison de suppression et leur date d'ajout. Les options suivantes sont disponibles :

   a. Sélectionnez une adresse e-mail ou cochez la case correspondante et choisissez View report (Afficher le rapport) pour en afficher les détails. (S'il s'agit d'une adresse qui a été automatiquement ajoutée à votre liste de suppression en raison d'un retour à l'expéditeur ou d'une réclamation, des informations seront affichées sur l'événement de commentaires qui a provoqué son ajout, y compris des détails sur le message de l'e-mail qui a produit l'événement déclencheur.)

   b. Vous pouvez personnaliser le tableau de la liste de suppression en choisissant l'icône en forme d'engrenage. Un modal sera présenté dans lequel vous pourrez personnaliser la taille de la page, le retour à la ligne et les colonnes à afficher. Après avoir effectué vos

sélections, choisissez Confirm (Confirmer). Le tableau de liste de suppression reflétera vos choix d'affichage.

Retrait d'adresses e-mail individuelles de la liste de suppression au niveau de votre compte Amazon SES

Si une adresse est sur la liste de suppression de votre compte, mais que vous savez qu'elle ne doit pas y figurer, vous pouvez la supprimer via l'opération DeleteSuppressedDestination de l'API SES v2.

> **Note**
>
> La procédure suivante suppose que vous avez déjà installé le AWS CLI. Pour en savoir plus sur l'installation et la configuration de l'AWS CLI, consultez le Guide de l'utilisateur de l'AWS Command Line Interface.

Pour supprimer des adresses individuelles de la liste de suppression au niveau de votre compte à l'aide de l'AWS CLI

- Sur la ligne de commande, entrez la commande suivante :

  Linux, macOS, or Unix

  ```
  aws sesv2 delete-suppressed-destination \
  --email-address recipient@example.com
  ```

  Windows

  ```
  aws sesv2 delete-suppressed-destination `
  --email-address recipient@example.com
  ```

  Dans l'exemple précédent, remplacez *recipient@example.com* par l'adresse e-mail que vous souhaitez supprimer de la liste de suppression au niveau de votre compte.

Pour supprimer des adresses individuelles de la liste de suppression au niveau de votre compte à l'aide de la console SES :

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES sur la page https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Suppression list (Liste de suppression).
3. Supprimez les adresses e-mail individuelles soit par (a) sélection de table, soit par (b) saisie :

    a. Sélectionner depuis la table : dans la table Suppression list (Liste de suppression), cochez la case correspondante d'une ou de plusieurs adresses e-mail et choisissez Remove (Supprimez).

    b. Saisie dans le champ :

        i. Dans la table Suppression list (Liste de suppression), choisissez Remove email address (Supprimer l'adresse e-mail).

        ii. Saisissez une adresse e-mail dans le champ Email address (Adresse e-mail). Si vous devez saisir d'autres adresses, choisissez Enter another address (Saisir une autre adresse) et répétez l'opération pour chaque adresse supplémentaire.

        iii. Lorsque vous avez terminé de saisir les adresses, vérifiez la précision de vos entrées. Si vous décidez que l'une de vos entrées ne doit pas faire partie de cette soumission, cliquez sur le bouton Remove (Supprimer).

        iv. Choisissez Save changes (Enregistrer les modifications) pour supprimer les adresses e-mail saisies de votre liste de suppression au niveau du compte.

Retrait d'adresses e-mail en bloc de la liste de suppression au niveau de votre compte Amazon SES

Vous pouvez supprimer des adresses en bloc en chargeant d'abord votre liste de contacts dans un objet Amazon S3, puis en utilisant l'opération CreateImportJob dans l'API SES v2.

> **Note**
>
> - Le nombre d'adresses que vous pouvez retirer de la liste de suppression au niveau du compte n'est pas limité, mais il existe une limite de suppression de 10 000 d'adresses dans un objet Amazon S3 par appel d'API.

- Si votre source de données est un compartiment S3, celui-ci doit se trouver dans la région où vous effectuez l'importation.

Pour retirer des adresses e-mail en bloc de votre liste de suppression au niveau du compte, procédez comme suit.

- Téléchargez votre liste d'adresses dans un objet Amazon S3 au format CSV ou JSON.

  Exemple de format CSV pour retirer des adresses :

  recipient3@example.com

  Seuls les nouveaux fichiers JSON délimités par une ligne sont pris en charge. Dans ce cas, chaque ligne est un objet JSON complet qui contient une définition d'adresse distincte.

  Exemple de format JSON pour ajouter des adresses :

  {"emailAddress":"*recipient3@example.com*"}

  Dans les exemples précédents, remplacez *recipient3@example.com* par les adresses e-mail que vous souhaitez supprimer de la liste de suppression au niveau de votre compte.
- Autoriser SES à lire l'objet Amazon S3.

  Appliquée à un compartiment Amazon S3, la politique suivante accorde à SES l'autorisation de lire ce compartiment. Pour plus d'informations sur l'attachement de stratégies de compartiment vers Amazon S3, veuillez consulter Stratégies de compartiment et stratégies d'utilisateur dans le Guide de l'utilisateur d'Amazon Simple Storage Service.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSESGet",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::BUCKET-NAME/OBJECT-NAME",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:Referer": "AWSACCOUNTID"
                }
            }
        }
    ]
}
```

- Autoriser SES à utiliser votre clé AWS KMS.

  Si l'objet Amazon S3 est chiffré avec une clé AWS KMS, vous devez attribuer à Amazon SES l'autorisation d'utiliser la clé AWS KMS. SES ne peut obtenir l'autorisation qu'à partir d'une clé gérée par le client, et non d'une clé KMS par défaut. Vous devez accorder à SES l'autorisation d'utiliser la clé gérée par le client en ajoutant une instruction à la politique de la clé.

  Collez l'instruction de politique suivante dans la politique de clé pour permettre à SES d'utiliser votre clé gérée par le client.

```
{
   "Sid": "AllowSESToDecrypt",
   "Effect": "Allow",
   "Principal": {
       "Service":"ses.amazonaws.com"
   },
   "Action": [
       "kms:Decrypt",
   ],
   "Resource": "*"
}
```

- Utilisez l'opération CreateImportJob dans l'API SES v2.

> **Note**
>
> L'exemple suivant suppose que vous avez déjà installé le AWS CLI. Pour en savoir plus sur l'installation et la configuration de l'AWS CLI, consultez le Guide de l'utilisateur de l'AWS Command Line Interface.

En ligne de commande, entrez la commande suivante. Remplacez *s3bucket* par le nom du compartiment Amazon S3 et *s3object* par le nom de l'objet Amazon S3.

```
aws sesv2 create-import-job --import-destination
 SuppressionListDestination={SuppressionListImportAction=DELETE} --import-data-source
 S3Url="s3://s3bucket/s3object",DataFormat=CSV
```

Pour supprimer les adresses e-mail en bloc de la liste de suppression au niveau de votre compte à l'aide de la console SES :

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES sur la page https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Suppression list (Liste de suppression).
3. Dans Suppression list (Liste de suppression), développez le bouton Bulk actions (Actions en bloc) et sélectionnez Remove email addresses in bulk (Supprimer les adresses e-mail en bloc).
4. Dans Bulk action specifications (Spécifications de l'action en bloc), sélectionnez l'un des points (a) Choose file from S3 bucket (Choisir le fichier dans le compartiment S3) ou (b) Import From File (Importer depuis un fichier). Les procédures sont données pour chaque méthode d'importation :

    a. Choose file from S3 bucket (Choisir le fichier dans le compartiment S3) – si votre fichier source est déjà stocké dans un compartiment Amazon S3 :

        i. Si vous connaissez l'URI du compartiment Amazon S3 que vous souhaitez utiliser, saisissez-le dans le champ URI Amazon S3 ; sinon, choisissez Parcourir S3 :

            A. Dans Buckets (Compartiments), sélectionnez le nom du compartiment S3.

            B. Dans Objects (Objets), sélectionnez le nom du fichier, puis sélectionnez Choose (Choisir) – vous serez renvoyé à Bulk action specifications (Spécifications de l'action en bloc).

            C. (Facultatif) Si vous souhaitez être redirigé vers la console Amazon S3 pour afficher les détails de votre objet S3, choisissez View (Afficher).

        ii. Dans File format (Format de fichier), sélectionnez le format du fichier que vous avez choisi d'importer à partir de votre compartiment Amazon S3.

        iii. Choisissez Remove email addresses (Supprimer les adresses e-mail) pour lancer l'importation d'adresses depuis votre fichier – un tableau sous l'onglet Bulk actions (Actions en bloc) s'affiche.

b. Import From File (Importer depuis un fichier) – si vous avez un fichier source local à charger vers un compartiment Amazon S3 nouveau ou existant :

   i. Dans Import source file (Importer le fichier source), sélectionnez Choose file (Choisir le fichier).

   ii. Sélectionnez le fichier JSON ou CSV dans le navigateur de fichiers et choisissez Open (Ouvrir) – vous verrez le nom, la taille et la date de votre fichier s'affichent sous le bouton Choose file (Choisir le fichier).

   iii. Développer Amazon S3 bucket (Compartiment Amazon S3) et sélectionnez le compartiment S3.

      - Pour charger votre fichier dans un nouveau compartiment, choisissez Create S3 bucket (Créer un compartiment S3), saisissez un nom dans le Bucket name (Nom du compartiment) et choisissez Create bucket (Créer un compartiment).

   iv. Choisissez Remove email addresses (Supprimer les adresses e-mail) pour lancer l'importation d'adresses depuis votre fichier – un tableau sous l'onglet Bulk actions (Actions en bloc) s'affiche.

5. Quelle que soit la méthode d'importation que vous avez utilisée, votre ID de tâche sera répertorié dans Bulk actions (Actions en bloc) avec le type d'importation, le statut et la date – pour afficher les détails de la tâche, sélectionnez l'ID de tâche.

6. Sélectionnez l'onglet Suppression list (Liste de suppression) et toutes les adresses e-mail correctement importées qui ont été supprimées de votre liste de suppression ne seront plus affichées.

Affichage d'une liste de tâches d'importation pour le compte

Vous pouvez afficher une liste de toutes les adresses de messagerie figurant dans la liste de suppression au niveau de votre compte de votre compte à l'aide de l'opération ListImportJobs dans l'API Amazon SES v2.

> **Note**
>
> La procédure suivante suppose que vous avez déjà installé le AWS CLI. Pour en savoir plus sur l'installation et la configuration de l'AWS CLI, consultez le Guide de l'utilisateur de l'AWS Command Line Interface.

Pour afficher la liste de toutes les tâches d'importation pour le compte

- Sur la ligne de commande, entrez la commande suivante :

```
aws sesv2 list-import-jobs
```

La commande précédente renvoie toutes les tâches d'importation pour le compte. La sortie ressemble à l'exemple suivant :

```
{
    "ImportJobs": [
        {
            "CreatedTimestamp": 2020-07-31T06:06:55Z",
            "ImportDestination": {
                "SuppressionListDestination": {
                    "SuppressionListImportAction": "PUT"
                }
            },
            "JobStatus": "COMPLETED",
            "JobId": "755380d7-fbdb-4ed2-a9a3-06866220f5b5"
        },
        {
            "CreatedTimestamp": "2020-07-30T18:45:32Z",
            "ImportDestination": {
                "SuppressionListDestination": {
                    "SuppressionListImportAction": "DELETE"
                }
            },
            "JobStatus": "COMPLETED",
            "JobId": "076683bd-a7ee-4a40-9754-4ad1161ba8b6"
        },
        {
            "CreatedTimestamp": "2020-08-05T16:45:18Z",
            "ImportDestination": {
                "SuppressionListDestination": {
                    "SuppressionListImportAction": "PUT"
                }
            },
            "JobStatus": "COMPLETED",
            "JobId": "6e261869-bd30-4b33-b1f2-9e035a83a395"
        }
    ]
```

```
}
```

Pour afficher la liste de toutes les tâches d'importation du compte à l'aide de la console SES :

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES sur la page https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Suppression list (Liste de suppression).
3. Dans le panneau Suppression list (Liste de suppression), sélectionnez l'onglet Bulk actions (Actions en bloc).
4. Toutes les tâches d'importation seront répertoriées dans le Bulk actions (Actions en bloc) avec le type d'importation, le statut et la date.
5. Pour afficher les détails de la tâche, sélectionnez l'ID de tâche et les panneaux suivants s'affichent :

    a. Bulk action status (État de l'action en bloc) : affiche l'état général des tâches, l'heure et la date à laquelle elles ont été terminées, le nombre d'enregistrements importés et le nombre d'enregistrements qui n'ont pas réussi à importer.

    b. Bulk action details (Détails de l'action en bloc) : affiche l'ID de tâche, s'il a été utilisé pour ajouter ou supprimer des adresses, si le format de fichier était JSON ou CSV, l'URI du compartiment Amazon S3 où le fichier groupé a été stocké, ainsi que l'heure et la date de création de l'action groupée.

Obtention des informations sur une tâche d'importation pour le compte

Vous pouvez obtenir des informations sur une tâche d'importation pour le compte à l'aide de l'opération GetImportJob dans l'API Amazon SES v2.

> **Note**
>
> La procédure suivante suppose que vous avez déjà installé le AWS CLI. Pour en savoir plus sur l'installation et la configuration de l'AWS CLI, consultez le Guide de l'utilisateur de l'AWS Command Line Interface.

Pour obtenir des informations sur une tâche d'importation pour le compte

- Sur la ligne de commande, entrez la commande suivante :

```
aws sesv2 get-import-job --job-id JobId
```

La commande précédente renvoie des informations sur une tâche d'importation pour le compte. La sortie ressemble à l'exemple suivant :

```
{
    "ImportDataSource": {
        "S3Url": "s3://bucket/object",
        "DataFormat": "CSV"
    },
    "ProcessedRecordsCount": 2,
    "FailureInfo": {
        "FailedRecordsS3Url": "s3presignedurl"
    },
    "JobStatus": "COMPLETED",
    "JobId": "jobid",
    "CreatedTimestamp": "2020-08-12T17:05:15Z",
    "FailedRecordsCount": 1,
    "ImportDestination": {
        "SuppressionListDestination": {
            "SuppressionListImportAction": "PUT"
        }
    },
    "CompletedTimestamp": "2020-08-12T17:06:42Z"
}
```

Pour obtenir des informations sur une tâche d'importation pour le compte à l'aide de la console SES :

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES sur la page https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Suppression list (Liste de suppression).
3. Dans le panneau Suppression list (Liste de suppression), sélectionnez l'onglet Bulk actions (Actions en bloc).

4. Toutes les tâches d'importation seront répertoriées dans le Bulk actions (Actions en bloc) avec le type d'importation, le statut et la date.
5. Pour afficher les détails de la tâche, sélectionnez l'ID de tâche et les panneaux suivants s'affichent :

    a. Bulk action status (État de l'action en bloc) : affiche l'état général des tâches, l'heure et la date à laquelle elles ont été terminées, le nombre d'enregistrements importés et le nombre d'enregistrements qui n'ont pas réussi à importer.

    b. Bulk action details (Détails de l'action en bloc) : affiche l'ID de tâche, s'il a été utilisé pour ajouter ou supprimer des adresses, si le format de fichier était JSON ou CSV, l'URI du compartiment Amazon S3 où le fichier groupé a été stocké, ainsi que l'heure et la date de création de l'action groupée.

Désactivation de la liste de suppression au niveau du compte Amazon SES

Vous pouvez utiliser l'opération PutAccountSuppressionAttributes dans l'API SES v2 pour désactiver efficacement la liste de suppression au niveau de votre compte en supprimant les valeurs de l'attribut `suppressed-reasons`.

> **Note**
>
> La procédure suivante suppose que vous avez déjà installé le AWS CLI. Pour en savoir plus sur l'installation et la configuration de l'AWS CLI, consultez le Guide de l'utilisateur de l'AWS Command Line Interface.

Pour désactiver la liste de suppression au niveau de votre compte à l'aide de l' AWS CLI

- Sur la ligne de commande, entrez la commande suivante :

```
aws sesv2 put-account-suppression-attributes --suppressed-reasons
```

Pour désactiver la liste de suppression au niveau de votre compte à l'aide de la console SES :

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES sur la page https://console.aws.amazon.com/ses/.

2. Dans le panneau de navigation, sous Configuration, choisissez Suppression list (Liste de suppression).
3. Dans Account-level settings (Paramètres au niveau du compte), choisissez Edit (Modifier).
4. Dans Suppression list (Liste de suppression), décochez la case Enabled (Activé).
5. Choisissez Enregistrer les modifications.

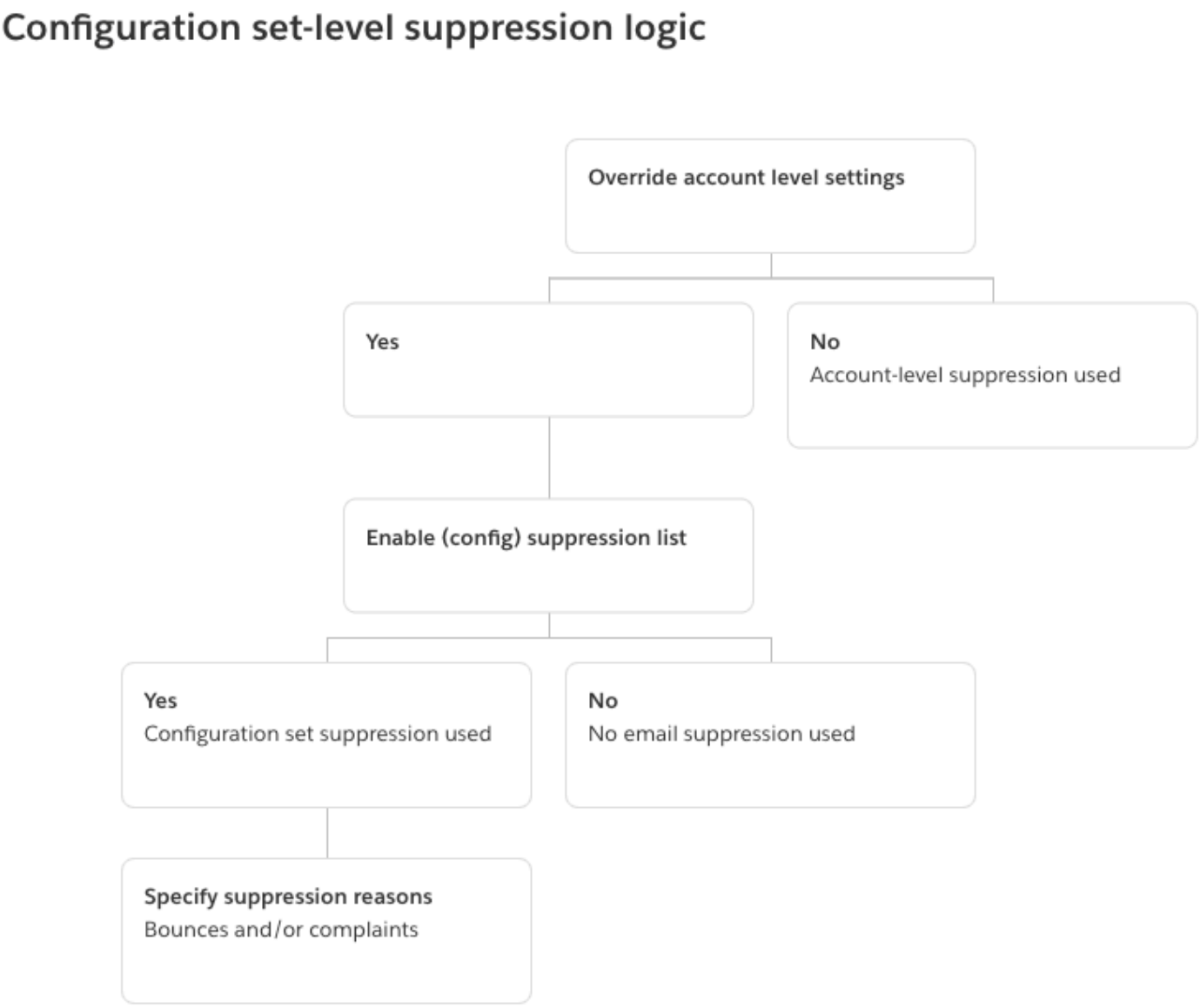
Utilisation de la suppression au niveau du jeu de configurations pour remplacer votre liste de suppression au niveau du compte

Bien que la liste de suppression au niveau du compte soit définie pour l'ensemble de votre compte, vous pouvez la personnaliser séparément pour différents jeux de configurations en la remplaçant par une suppression au niveau du jeu de configurations. Cette granularité plus fine vous permet d'utiliser des paramètres de suppression personnalisés pour différents groupes d'envoi d'e-mails que vous avez affectés à leurs propres jeux de configuration. Par exemple, supposons que votre liste de suppression au niveau du compte soit configurée pour ajouter des adresses de rebond et des adresses de réclamation, mais que vous disposiez d'une démographie de messagerie spécifique définie dans un ensemble de configuration pour lequel vous êtes uniquement intéressé par l'ajout d'adresses de réclamation. Vous pouvez y parvenir en activant les remplacements de suppression de ce jeu de configurations de sorte que les adresses e-mail soient ajoutées à votre liste de suppression au niveau du compte uniquement pour les plaintes (et non les retours à l'expéditeur et les plaintes comme dans votre liste de suppression au niveau du compte) à partir du courrier électronique envoyé avec ce jeu de configurations.

Avec la suppression au niveau du jeu de configurations, il existe différents niveaux de suppression au niveau du compte, y compris la possibilité de ne pas utiliser de suppression du tout. Pour aider à comprendre ces différents niveaux de suppression qui peuvent être définis dans les procédures de console suivantes, la carte de relations suivante modélise l'ensemble des choix que vous pouvez faire pour l'activation ou la désactivation de différents niveaux de dérogations, qui, selon leur combinaison, peuvent être utilisés pour mettre en œuvre trois niveaux différents de suppression.

- Pas de remplacements (par défaut) : le jeu de configurations utilise les paramètres de votre liste de suppression au niveau du compte.
- Remplacer les paramètres au niveau du compte : cela annulera tous les paramètres de liste de suppression au niveau du compte ; les e-mails envoyés avec ce jeu de configurations n'utiliseront aucun paramètre de suppression.

- Remplacer les paramètres au niveau du compte avec la suppression au niveau du jeu de configurations activée : les e-mails envoyés avec ce jeu de configurations utiliseront uniquement les conditions de suppression que vous avez activées pour lui (retours à l'expéditeur, plaintes ou retours à l'expéditeur et plaintes). Quels que soient les paramètres de votre liste de suppression au niveau du compte, ils les remplaceront.



N'oubliez pas que la suppression au niveau du jeu de configurations n’est pas une véritable liste de suppression, mais plutôt un mécanisme qui permet de remplacer votre liste de suppression au niveau du compte avec des paramètres de suppression personnalisés définis dans un jeu de configurations. Cela signifie que tout e-mail envoyé avec le jeu de configurations n’utilisera que

ses propres paramètres de suppression et ignorera les paramètres de suppression au niveau du compte. En d'autres termes, la suppression au niveau du jeu de configurations interagit avec votre liste de suppression au niveau du compte en modifiant simplement (en remplaçant) les raisons de suppression qui déterminent les adresses e-mail ajoutées à votre liste de suppression au niveau de votre compte.

Activer la suppression au niveau du jeu de configurations

Pour activer la suppression au niveau du jeu de configurations à l'aide de la nouvelle console Amazon SES :

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, sous Configuration, choisissez Configuration sets (Jeux de configurations).
3. Dans Jeux de configurations, choisissez le nom du jeu de configurations que vous souhaitez configurer avec une suppression personnalisée.
4. Dans Suppression list options (Options de liste de suppression), choisissez Edit (Modifier).
5. La section Suppression list options (Options de liste de suppression) fournit un ensemble de décisions permettant de définir une suppression personnalisée en commençant par l'option permettant d'utiliser ce jeu de configurations pour supplanter la suppression au niveau de votre compte. La carte logique de suppression au niveau du jeu de configurations vous aidera à comprendre les effets des combinaisons de remplacement. Ces sélections à plusieurs niveaux de remplacement peuvent être combinées pour implémenter trois niveaux de suppression différents :

   a. Use account-level suppression (Utiliser la suppression au niveau du compte) : ne remplace pas la suppression au niveau de votre compte et n'implémente aucune suppression au niveau du jeu de configurations. En fait, tout e-mail envoyé à l'aide de ce jeu de configurations utilisera simplement la suppression au niveau de votre compte. Pour cela :

      - Dans Suppression list settings (Paramètres de la liste de suppression), décochez la case Override account level settings (Remplacer les paramètres au niveau du compte).

   b. Do not use any suppression (N'utiliser aucune suppression) : remplace la suppression au niveau de votre compte sans activer la suppression au niveau du jeu de configurations. Cela signifie que tout e-mail envoyé à l'aide de ce jeu de configurations n'utilisera aucune

suppression au niveau de votre compte ; en d'autres termes, toute suppression est annulée. Pour cela :

i. Dans Suppression list settings (Paramètres de la liste de suppression), cochez la case Override account level settings (Remplacer les paramètres au niveau du compte).

ii. Dans Suppression list (Liste de suppression), décochez la case Enabled (Activé).

c. Use configuration set-level suppression (Utiliser la suppression au niveau du jeu de configurations) : remplace la suppression au niveau de votre compte par des paramètres de suppression personnalisés définis dans ce jeu de configurations. Cela signifie que tout e-mail envoyé à l'aide de ce jeu de configurations utilisera uniquement ses propres paramètres de suppression et ignorera tous les paramètres de suppression au niveau du compte. Pour cela :

i. Dans Suppression list settings (Paramètres de la liste de suppression), cochez la case Override account level settings (Remplacer les paramètres au niveau du compte).

ii. Dans Suppression list (Liste de suppression), cochez la case Enabled (Activé).

iii. Dans Specify the reason(s)... (Spécifiez la ou les raisons...), sélectionnez l'un des motifs de suppression à utiliser pour ce jeu de configurations.

6. Choisissez Enregistrer les modifications.

Utilisation de la gestion des listes

Amazon SES offre des fonctionnalités de gestion des listes, ce qui signifie que les clients peuvent gérer leurs propres listes de diffusion, appelées listes de contacts. Une liste de contacts est une liste qui vous permet de stocker tous vos contacts qui se sont abonnés à une ou plusieurs rubriques particulières. Un contact est un utilisateur final qui reçoit vos e-mails. Une rubrique est un groupe d'intérêt, un thème ou un libellé au sein d'une liste. Les listes peuvent avoir plusieurs rubriques.

En utilisant l'opération `ListContacts` dans l'API Amazon SES v2, vous pouvez récupérer une liste de tous vos contacts qui se sont abonnés à une rubrique particulière, et auxquels vous pouvez envoyer des e-mails à l'aide de l'opération `SendEmail`.

Pour en savoir plus sur la gestion des abonnements, consultez la page Utilisation de la gestion des abonnements.

Présentation de la gestion des listes

Vous devez tenir compte des facteurs suivants lorsque vous utilisez la gestion des listes :

- Vous pouvez spécifier des rubriques de liste lors de la création de la liste.
- Une seule liste de contacts est autorisée par Compte AWS.
- Une liste peut comporter un maximum de 20 rubriques.
- Vous pouvez mettre à jour une liste de contacts existante, y compris ajouter de nouvelles rubriques à la liste, ajouter ou supprimer des contacts d'une liste et mettre à jour des préférences de contact pour une liste ou une rubrique.
- Vous pouvez mettre à jour les métadonnées d'une rubrique, telles que le nom d'affichage ou la description de la rubrique.
- Vous pouvez obtenir une liste de contacts dans une liste de contacts, de contacts abonnés à une rubrique, de contacts désabonnés d'une rubrique et de contacts désabonnés de toutes les rubriques de la liste.
- Vous pouvez importer vos listes de contacts existantes dans Amazon SES à l'aide de l'API `CreateImportJob`.
- Amazon SES retournera un e-mail à l'expéditeur s'il est envoyé à un contact désabonné de votre liste de contacts. Pour de plus amples informations, veuillez consulter Utilisation de la gestion des abonnements.
- Chaque contact peut avoir des attributs associés que vous pouvez utiliser pour stocker des informations sur ce contact.

Configuration de la gestion des listes

Vous pouvez utiliser les opérations suivantes pour configurer les capacités de gestion des listes. Pour obtenir la liste complète des opérations de liste de contacts et de contact, consultez le document Référence de l'API Amazon SES v2.

Création d'une liste de contacts

Vous pouvez utiliser l'opération `CreateContactList` dans l'API Amazon SES v2 pour créer une liste de contacts. Vous pouvez configurer rapidement et facilement ce paramètre en utilisant l' AWS CLI. Pour en savoir plus sur l'installation et la configuration de l'AWS CLI, consultez le Guide de l'utilisateur de l'AWS Command Line Interface.

Pour créer une liste de contacts à l'aide de l'AWS CLI

- Sur la ligne de commande, entrez la commande suivante :

```
aws sesv2 create-contact-list --cli-input-json file://CONTACT-LIST-JSON
```

Dans la commande précédente, remplacez *CONTACT-LIST-JSON* par le chemin de votre fichier JSON pour votre demande `CreateContactList`.

Un exemple de fichier JSON d'entrée `CreateContactList` pour la demande est le suivant :

```
{
    "ContactListName": "ExampleContactListName",
    "Description": "Creating a contact list example",
    "Topics": [
     {
         "TopicName": "Sports",
         "DisplayName": "Sports Newsletter",
         "Description": "Sign up for our free newsletter to receive updates on all
 sports.",
         "DefaultSubscriptionStatus": "OPT_OUT"
     },
     {
         "TopicName": "Cycling",
         "DisplayName": "Cycling newsletter",
         "Description": "Never miss a cycling update by subscribing to our
 newsletter.",
         "DefaultSubscriptionStatus": "OPT_IN"
     },
     {
         "TopicName": "NewProducts",
         "DisplayName": "New products",
         "Description": "Hear about new products by subscribing to this mailing
 list.",
         "DefaultSubscriptionStatus": "OPT_IN"
     },
     {
         "TopicName": "DailyUpdates",
         "DisplayName": "Daily updates",
         "Description": "Start your day with sport updates, Monday through
 Friday.",
         "DefaultSubscriptionStatus": "OPT_OUT"
```

```
     }
    ]
}
```

Créer un contact

Vous pouvez utiliser l'opération `CreateContact` dans l'API Amazon SES v2 pour créer un contact. Vous pouvez configurer rapidement et facilement ce paramètre en utilisant l' AWS CLI. Pour en savoir plus sur l'installation et la configuration de l'AWS CLI, consultez le Guide de l'utilisateur de l'AWS Command Line Interface.

Pour créer un contact à l'aide de l'AWS CLI

- Sur la ligne de commande, entrez la commande suivante :

  ```
  aws sesv2 create-contact --cli-input-json file://CONTACT-JSON
  ```

  Dans la commande précédente, remplacez *CONTACT-JSON* par le chemin de votre fichier JSON pour votre demande `CreateContact`.

  Un exemple de fichier JSON d'entrée `CreateContact` pour la demande est le suivant :

  ```
  {
      "ContactListName": "ExampleContactListName",
      "EmailAddress": "example@amazon.com",
      "UnsubscribeAll": false,
      "TopicPreferences": [
          {
              "TopicName": "Sports",
              "SubscriptionStatus": "OPT_IN"
          }
      ],
      "AttributesData": "{\"Name\": \"John\", \"Location\": \"Seattle\"}"
  }
  ```

  Dans l'exemple ci-dessus, une valeur `UnsubscribeAll` de `false` indique que le contact ne s'est pas désabonné de toutes les rubriques, tandis qu'une valeur de `true` signifierait que le contact s'est désabonné de toutes les rubriques.

`TopicPreferences` inclut des informations sur le statut d'abonnement du contact aux rubriques. Dans l'exemple précédent, le contact a opté pour la rubrique « Sports » et recevra tous les e-mails la concernant.

`AttributesData` est un champ JSON dans lequel vous pouvez placer des métadonnées sur notre contact. Il doit s'agir d'un objet JSON valide.

Importation de contacts en bloc dans votre liste de contacts

Vous pouvez ajouter manuellement des adresses en bloc en téléchargeant d'abord vos contacts dans un objet Amazon S3, puis en utilisant l'opération `CreateImportJob` dans l'API Amazon SES v2. Pour plus d'informations, consultez Ajout d'adresses e-mail en bloc à la liste de suppression au niveau de votre compte.

Vous devez créer une liste de contacts avant d'importer vos contacts.

> **Note**
>
> Vous pouvez ajouter jusqu'à un million de contacts à une liste de contacts par ImportJob.

Pour ajouter des contacts en bloc à votre liste de contacts, procédez comme suit.

- Téléchargez vos contacts dans un objet Amazon S3 au format CSV ou JSON.

  Format CSV

  La première ligne du fichier téléchargée sur Amazon S3 doit être une ligne d'en-tête.

  L'objet `topicPreferences` doit être réduit pour le format CSV. Chaque rubrique du `topicPreferences` aura un champ d'en-tête distinct.

  Exemple de format CSV pour ajouter des contacts en bloc à une liste de contacts :

```
emailAddress,unsubscribeAll,attributesData,topicPreferences.Sports,topicPreferences.Cycling
example1@amazon.com,false,{"Name": "John"},OPT_IN,OPT_OUT
example2@amazon.com,true,,OPT_OUT,OPT_OUT
```

Format JSON

Seuls les nouveaux fichiers JSON délimités par une ligne sont pris en charge. Dans ce cas, chaque ligne est un objet JSON complet qui contient les informations d'un contact.

Exemple de format JSON pour ajouter des contacts en bloc à une liste de contacts :

```
{
     "emailAddress": "example1@amazon.com",
     "unsubscribeAll": false,
     "attributesData": "{\"Name\":\"John\"}",
     "topicPreferences": [
      {
          "topicName": "Sports",
          "subscriptionStatus": "OPT_IN"
      },
      {
          "topicName": "Cycling",
          "subscriptionStatus": "OPT_OUT"
      }
     ]
}
{
     "emailAddress": "example2@amazon.com",
     "unsubscribeAll": true,
     "topicPreferences": [
      {
          "topicName": "Sports",
          "subscriptionStatus": "OPT_OUT"
      },
      {
          "topicName": "Cycling",
          "subscriptionStatus": "OPT_OUT"
      }
     ]
}
```

Dans les exemples précédents, remplacez *example1@amazon.com* et *example2@amazon.com* par les adresses e-mail que vous souhaitez ajouter à la liste de contacts. Remplacez les

valeurs `attributesData` par les valeurs spécifiques au contact. En outre, remplacez *`Sport`* et *`Cyclisme`* par la valeur `topicName` qui s'applique à votre contact. Les objets `topicPreferences` acceptables sont *`OPT_IN`* et *`OPT_OUT`*.

Les attributs suivants sont pris en charge lors du téléchargement de vos contacts dans un objet Amazon S3 au format CSV ou JSON :

Attribut	Description
`emailAddress`	Adresse e-mail du contact. Ce champ est obligatoire.
`unsubscribeAll`	Statut de valeur booléenne indiquant si le contact est désabonné de toutes les rubriques de la liste de contacts.
`topicPreferences`	Préférences du contact quant à l'abonnement ou non aux rubriques.
`attributesData`	Données d'attribut attachées à un contact.

- Autoriser Amazon SES à lire l'objet Amazon S3.

  Appliquée à un compartiment Amazon S3, la stratégie suivante donne à Amazon SES l'autorisation de lire ce compartiment. Pour de plus amples informations sur l'attachement de stratégies de compartiment vers Amazon S3, veuillez consulter Stratégies de compartiment et stratégies d'utilisateur dans le Guide de l'utilisateur d'Amazon Simple Storage Service.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSESGet",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::BUCKET-NAME/OBJECT-NAME",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:Referer": "AWSACCOUNTID"
                }
            }
        }
    ]
}
```

- Attribuer à Amazon SES l'autorisation d'utiliser votre clé AWS KMS

  Si l'objet Amazon S3 est chiffré avec une clé AWS KMS, vous devez attribuer à Amazon SES l'autorisation d'utiliser la clé KMS. Amazon SES ne peut obtenir l'autorisation qu'à partir d'une clé gérée par le client, et non d'une clé KMS par défaut. Vous devez donner à Amazon SES la permission d'utiliser la clé gérée par le client en ajoutant une déclaration à la stratégie de la clé.

  Collez la déclaration de stratégie suivante dans la stratégie de clé pour autoriser Amazon SES à utiliser votre clé gérée par le client.

```
{
   "Sid": "AllowSESToDecrypt",
   "Effect": "Allow",
   "Principal": {
       "Service":"ses.amazonaws.com"
   },
   "Action": [
       "kms:Decrypt",
   ],
   "Resource": "*"
}
```

- Utilisez l'opération `CreateImportJob` dans l'API Amazon SES v2.

> **Note**
>
> L'exemple suivant suppose que vous avez déjà installé le AWS CLI. Pour en savoir plus sur l'installation et la configuration de l'AWS CLI, consultez le Guide de l'utilisateur de l'AWS Command Line Interface.

En ligne de commande, entrez la commande suivante. Remplacez *s3bucket* par le nom du compartiment Amazon S3 et *s3object* par le nom de l'objet Amazon S3.

```
aws sesv2 create-import-job --import-destination
 ContactListDestination={ContactListName=ExampleContactListName,ContactListImportAction=PUT}
 --import-data-source S3Url="s3://s3bucket/s3object",DataFormat=CSV
```

Procédure pas à pas de gestion des listes avec des exemples

La procédure pas à pas suivante fournit des exemples de la façon dont vous pouvez utiliser la gestion des listes pour répertorier vos contacts et `ListManagementOptions` pour spécifier une liste de contacts et un nom de sujet dans votre e-mail. Elle indique également comment insérer des liens de désabonnement.

1. Répertorier les contacts en utilisant AWS CLI – Vous pouvez utiliser l'opération `ListContacts` pour récupérer une liste de tous vos contacts qui se sont abonnés à une rubrique particulière, parallèlement à l'opération`SendEmail` , qui vous permet de leur envoyer des e-mails.

   Sur la ligne de commande, entrez la commande suivante :

   ```
   aws sesv2 list-contacts --cli-input-json file://LIST-CONTACTS-JSON
   ```

   Dans la commande précédente, remplacez *`LIST-CONTACTS-JSON`* par le chemin de votre fichier JSON pour votre demande `ListContacts`.

   Un exemple de fichier JSON d'entrée `ListContacts` pour la demande est le suivant :

   ```
   {
       "ContactListName": "ExampleContactListName",
       "Filter": {
           "FilteredStatus": "OPT_IN",
           "TopicFilter": {
               "TopicName": "Cycling",
               "UseDefaultIfPreferenceUnavailable": true
           }
       },
       "PageSize": 50
   }
   ```

   Le paramètre `FilteredStatus` affiche l'état d'abonnement pour lequel vous souhaitez appliquer un filtre, qui est soit `OPT_IN`, soit `OPT_OUT`.

Le filtre `TopicFilter` est un filtre facultatif qui spécifie la rubrique pour laquelle vous souhaitez obtenir des résultats, à savoir « Cyclisme » dans l'exemple ci-dessus.

`UseDefaultIfPreferenceUnavailable` peut avoir la valeur `true` ou `false`. S'il s'agit de `true`, la préférence de rubrique par défaut sera utilisée si le contact n'a aucune préférence explicite pour une rubrique. S'il s'agit de `false`, seuls les contacts qui ont une préférence explicitement définie sont pris en compte pour le filtrage.

2. Envoyer un e-mail avec **`ListManagementOptions`** activé – Après avoir répertorié les contacts dans votre liste à l'aide de l'opération `ListContacts` ci-dessus, vous pouvez utiliser l'opération `SendEmail` pour envoyer des e-mails à chacun de vos contacts à l'aide de l'en-tête `ListManagementOptions` afin de spécifier votre liste de contacts et votre nom de rubrique.

   Pour utiliser `ListManagementOptions` avec l'opération `SendEmail`, incluez `contactListName` et `topicName` auxquels appartient l'e-mail (`topicNameest` facultatif) :

   ```
   ListManagementOptions:
       String contactListName
       String topicName
   ```

   Si vous incluez `ListManagementOptions` dans votre demande `SendEmail` à une adresse e-mail de destinataire qui ne figure pas sur votre liste de contacts, un contact sera automatiquement créé dans votre liste.

   Amazon SES renverra un e-mail à l'expéditeur s'il est envoyé à un contact désabonné de votre liste de contacts, ce qui signifie que vous n'aurez pas besoin de mettre à jour vos demandes `SendEmail` pour éviter de les envoyer à des contacts qui se sont désabonnés.

3. Indiquer l'emplacement de vos liens de désabonnement – Lorsque vous utilisez `ListManagementOptions`, vous avez la possibilité d'autoriser Amazon SES à ajouter des liens de bas de page de désabonnement dans votre e-mail à l'aide de l'espace réservé `{{amazonSESUnsubscribeUrl}}` pour spécifier où SES doit insérer l'URL de désabonnement. Le remplacement des espaces réservés n'est pris en charge que pour les types de contenu HTML et TEXT. Vous pouvez inclure l'espace réservé deux fois maximum. S'il est utilisé plus de deux fois, seules les deux premières occurrences sont remplacées. Pour de plus amples informations, veuillez consulter Utilisation de la gestion des abonnements.

Vous pouvez également utiliser l'en-tête `X-SES-LIST-MANAGEMENT-OPTIONS` pour spécifier une liste et un nom de rubrique si vous utilisez l'interface SMTP pour envoyer des e-mails.

Pour spécifier une liste et un nom de rubrique lors de l'envoi d'e-mails à l'aide de l'interface SMTP, ajoutez l'en-tête d'e-mail suivant à votre message :

```
X-SES-LIST-MANAGEMENT-OPTIONS: {contactListName}; topic={topicName}
```

Utilisation de la gestion des abonnements

Amazon SES fournit une fonctionnalité de gestion des abonnements, dans laquelle Amazon SES active automatiquement les liens de désabonnement dans chaque e-mail sortant lorsque vous spécifiez `contactListName` et `topicName` dans `ListManagementOptions` dans la demande d'opération `SendEmail`.

Si un contact se désabonne d'une rubrique ou d'une liste particulière, Amazon SES n'autorise pas l'envoi d'e-mails au contact pour cette rubrique ou cette liste à l'avenir.

> **Note**
>
> - La gestion des abonnements Amazon SES prend en charge les exigences relatives aux expéditeurs groupés, telles qu'elles sont imposées par de nombreux fournisseurs de services de messagerie. Consultez la section 2 de la section Présentation des modifications apportées aux expéditeurs groupés pour plus d'informations.
> - La gestion des abonnements est disponible pour ceux qui utilisent Easy DKIM dans Amazon SES, mais Amazon SES ne peut pas ajouter les liens de désabonnement à votre e-mail pour les expéditeurs qui signent eux-mêmes des e-mails avant d'appeler Amazon SES.

Pour de plus amples informations sur la gestion des listes et sur la façon de l'utiliser, y compris pour récupérer une liste de tous vos contacts qui se sont abonnés à une rubrique particulière, veuillez consulter Utilisation de la gestion des listes.

Présentation de la gestion des abonnements

Vous devez tenir compte des facteurs suivants lorsque vous utilisez la gestion des abonnements :

- La gestion des abonnements sera entièrement gérée par Amazon SES. Cela signifie qu'Amazon SES reçoit des e-mails et des demandes de désabonnement à partir de la page web de désabonnement, puis met à jour la préférence du contact dans votre liste. Vous pouvez recevoir des notifications de désabonnement à l'aide des notifications de jeu de configurations. Pour en savoir plus sur les jeux de configurations, consultez Utilisation des jeux de configuration dans Amazon SES.
- Vous devez spécifier la liste de contacts lors de l'envoi de l'e-mail. La gestion des abonnements via les liens d'en-tête `List-Unsubscribe` et le pied de page `ListManagementOptions` sera gérée en conséquence.
- Amazon SES ajoute la prise en charge des normes d'en-tête `List-Unsubscribe`, qui permettront aux clients de messagerie et aux fournisseurs de boîte de réception d'afficher un lien de désabonnement en haut de l'e-mail s'ils le prennent en charge. Certains fournisseurs de services de messagerie ne prennent pas en charge ces en-têtes.
- Les en-têtes `List-Unsubscribe` adoptent le comportement suivant :
  - Si un contact clique sur le lien d'en-tête de désabonnement dans un e-mail qui contient à la fois la liste des contacts et la rubrique spécifiées, le contact ne sera désabonné que de cette rubrique spécifique.
  - Si la rubrique n'est pas spécifiée, le contact sera désabonné de toutes les rubriques de la liste.
- Les contacts seront redirigés vers une page de destination de désabonnement lorsqu'ils cliquent sur un lien de désabonnement dans le pied de page de l'e-mail.
- La page de destination de désabonnement donnera aux contacts une option pour mettre à jour leurs préférences, soit `OPT_IN` ou `OPT_OUT`, pour toutes les rubriques d'une liste particulière. La page de destination permet également de se désabonner de toutes les rubriques de la liste.
- Si vous utilisez `ListManagementOptions`, vous devez inclure un espace réservé dans vos e-mails pour indiquer où Amazon SES doit insérer l'URL de désabonnement. Vous pouvez inclure l'espace réservé deux fois maximum. S'il est utilisé plus de deux fois, seules les deux premières occurrences sont remplacées.
- Les liens d'en-tête `List-Unsubscribe` et de pied de page `ListManagementOptions` ne sont ajoutés que si l'e-mail est envoyé à un seul destinataire.
- Pour les e-mails transactionnels où vous ne souhaitez pas que les contacts puissent se désabonner, vous pouvez omettre le champ `ListManagementOptions` avec votre demande `SendEmail`.

Considérations relatives à l'en-tête de désabonnement

La gestion des abonnements via un lien de désabonnement est activée lorsque l'e-mail contient les en-têtes suivants :

`List-Unsubscribe`

`List-Unsubscribe-Post`

Lorsque vous utilisez la gestion des abonnements Amazon SES,`ListManagementOptions`, Amazon SES remplacera ces en-têtes s'ils sont présents dans l'e-mail.

Les destinataires qui se désabonnent en cliquant sur le lien produit par ces en-têtes auront une expérience différente en fonction de leur client de messagerie ou de leur fournisseur de boîte de réception, car certains fournisseurs ne reconnaissent pas les en-têtes `List-Unsubscribe` et `List-Unsubscribe-Post` ; les e-mails envoyés aux destinataires utilisant ces fournisseurs ne verront pas le lien Se désabonner.

Les destinataires dont le client de messagerie reconnaît ces en-têtes verront le lien Se désabonner avec lequel ils pourront se désabonner, mais ils n'auront pas la possibilité de choisir les rubriques dont ils se désabonnent. Ils seront simplement désabonnés de la rubrique pour laquelle l'e-mail a été envoyé.

Pour de plus amples informations sur l'en-tête `List-Unsubscribe`, consultez RFC 2369, et pour l'en-tête `List-Unsubscribe-Post`, consultez RFC 8058.

> **Note**
>
> Amazon SES prend en charge le désabonnement en un clic conformément aux exigences relatives aux expéditeurs groupés, telles qu'appliquées par de nombreux fournisseurs de services de messagerie. Consultez Utiliser le désabonnement en un clic avec Amazon SES pour plus d'informations.

Ajout d'un lien de pied de page de désabonnement

Vous devrez utiliser l'espace réservé `{{amazonSESUnsubscribeUrl}}` dans les e-mails modélisés et non modélisés pour spécifier où Amazon SES doit insérer l'URL de désabonnement.

Le remplacement des espaces réservés n'est pris en charge que pour les types de contenu HTML et TEXT.

Vous pouvez inclure l'espace réservé deux fois maximum. S'il est utilisé plus de deux fois, seules les deux premières occurrences sont remplacées.

> **Note**
>
> L'espace réservé `{{amazonSESUnsubscribeUrl}}` ne peut être utilisé que si `ListManagementOptions` est spécifié en tant qu'en-tête lors de l'utilisation de l'opération `SendEmail` ou X-SES-LIST-MANAGEMENT-OPTIONS est spécifié en tant qu'en-tête lors de l'utilisation de l'interface SMTP. (A ne pas confondre avec les en-têtes `List-Unsubscribe` ou `List-Unsubscribe-Post` qui ne dépendent pas de `ListManagementOptions` et peuvent être utilisés par eux-mêmes.)

Surveillance de votre activité d'envoi Amazon SES

Amazon SES fournit des méthodes pour surveiller votre activité d'envoi à l'aide d'événements, de métriques et de statistiques. Un événement est un élément lié à votre activité d'envoi et dont vous avez décidé d'effectuer un suivi en tant que métrique. Une métrique représente un ensemble chronologique de points de données représentant les valeurs d'un type d'événement surveillé qui produit des statistiques. Les statistiques sont des regroupements de données métriques sur une durée spécifiée, y compris jusqu'à l'instant présent.

Ces méthodes de surveillance vous aident à suivre des métriques importantes, telles que les taux de retours à l'expéditeur, de réclamations et de rejets. Des taux trop élevés de retours à l'expéditeur et de réclamations peuvent compromettre votre capacité à envoyer des e-mails à l'aide de SES. Ces méthodes peuvent aussi être exploitées pour mesurer les taux d'interaction de vos clients avec les e-mails que vous envoyez, vous aidant ainsi à identifier vos taux globaux d'ouverture et de clics en utilisant la publication d'événements et des domaines personnalisés associés à des jeux de configuration (voir Configuration de domaines personnalisés pour gérer le suivi des ouvertures et des clics).

La première étape de la configuration de la surveillance consiste à identifier les types d'événements de messagerie liés à votre activité d'envoi que vous voulez mesurer et surveiller avec SES. Vous pouvez les types d'événement suivants à suivre dans SES :

- Send (Envoi) – La demande d'envoi a réussi et Amazon SES tente de remettre le message au serveur de messagerie du destinataire. (Si une suppression globale ou au niveau du compte est utilisée, SES la comptera toujours comme un envoi, mais la livraison sera supprimée).
- RenderingFailure— L'e-mail n'a pas été envoyé en raison d'un problème de rendu du modèle. Ce type d'événement peut se produire lorsqu'il manque des données du modèle ou lorsqu'il n'y a pas concordance entre les paramètres du modèle et les données. Ce type d'événement ne se produit que lorsque vous envoyez un e-mail à l'aide des opérations d'API `SendTemplatedEmail` ou `SendBulkTemplatedEmail`.
- Reject (Rejet) – Amazon SES a accepté l'e-mail, a déterminé qu'il contenait un virus et l'a rejeté. Amazon SES n'a pas tenté de remettre l'e-mail au serveur de messagerie du destinataire.
- Delivery (Livraison) – Amazon SES a bien remis l'e-mail au serveur de messagerie du destinataire.
- Bounce – Message d'erreur définitif indiquant que le serveur de messagerie du destinataire a définitivement rejeté l'e-mail. Les soft bounces (messages d'erreur temporaires) sont inclus

uniquement quand Amazon SES ne parvient pas à remettre l'e-mail après plusieurs tentatives au cours d'une période donnée.

- Complaint (Réclamation) – L'e-mail a été correctement remis au serveur de messagerie du destinataire, mais le destinataire l'a marqué comme courrier indésirable.
- DeliveryDelay— L'e-mail n'a pas pu être remis au serveur de messagerie du destinataire en raison d'un problème temporaire. Des retards de livraison peuvent se produire, par exemple lorsque la boîte de réception du destinataire est pleine ou lorsque le serveur de messagerie de réception rencontre un problème transitoire.
- Subscription (Abonnement) – L'e-mail a été envoyé avec succès, mais le destinataire a mis à jour les préférences d'abonnement en cliquant sur `List-Unsubscribe` dans l'en-tête de l'e-mail ou le lien `Unsubscribe` dans le pied-de-page.
- Open (Ouverture) – Le destinataire a reçu le message et l'a ouvert dans son client de messagerie.
- Click (Clic) – Le destinataire a cliqué sur un ou plusieurs liens contenus dans l'e-mail.

Vous pouvez surveiller les événements d'envoi d'e-mails de différentes manières. La méthode que vous choisissez dépend du type d'événement à surveiller, de la granularité et du niveau de détail souhaités et de l'endroit où Amazon SES devra publier les données. Vous devez utiliser les notifications de commentaires ou la publication d'événements pour suivre les événements de retour à l'expéditeur et de réclamation. Vous pouvez également choisir d'utiliser plusieurs méthodes de surveillance. Les caractéristiques de chaque méthode sont répertoriées dans le tableau suivant.

Méthode de surveillance	Événements que vous pouvez surveiller	Méthode d'accès aux données	Niveau de détail	Granularité
Console Amazon SES	État du compte, e-mails envoyés, quota utilisé, demandes d'envoi réussies, rejets, rebonds et réclamations (historique récent jusqu'à	Tableau de bord de compte de la console Amazon SES	Compte et pourcentage	Ensemble du compte AWS

Méthode de surveillance	Événements que vous pouvez surveiller	Méthode d'accès aux données	Niveau de détail	Granularité
	la réputation actuelle)			
Console Amazon SES	État du compte, e-mails envoyés, rebonds et réclamations (réputation actuelle)	Page métriques de réputation de la console Amazon SES	Taux calculés uniquement	Ensemble du compte AWS
API Amazon SES	Messages délivrés, retours à l'expéditeur, réclamations et rejets	`GetSendStatistics` Opérat d'API	Nombre uniquement	Ensemble du compte AWS

Méthode de surveillance	Événements que vous pouvez surveiller	Méthode d'accès aux données	Niveau de détail	Granularité
CloudWatch Console Amazon	Messages envoyés, messages livrés, messages ouverts, clics, retours à l'expéditeur, taux de retours à l'expéditeur, réclamations, taux de réclamations, rejets, échecs de rendu et adresses IP sur liste noire.	CloudWatch console **Note** Certaines mesures n'apparaissent pas CloudWatch tant que l'événement associé ne se produit pas. Par exemple, les métriques de rebond n'apparaissent que dans au moins un e-mail contenant des rebonds, ou	Nombre uniquement	Ensemble du compte AWS

Méthode de surveillance	Événements que vous pouvez surveiller	Méthode d'accès aux données	Niveau de détail	Granularité
		CloudWatch tant que vous n'avez pas généré un événement de rebond simulé à l'aide du simulateur de boîte aux lettres.		
Notifications de commentaire	Messages délivrés, retours à l'expéditeur et réclamations	Notification Amazon SNS (messages délivrés, retours à l'expéditeur et réclamations) ou e-mail (retours à l'expéditeur et réclamations uniquement). veuillez consulter Configuration des notifications d'événement par e-mail.	Détails sur chaque événement	Ensemble du compte AWS

Méthode de surveillance	Événements que vous pouvez surveiller	Méthode d'accès aux données	Niveau de détail	Granularité
Publication d'événement	Envois, messages délivrés, ouvertures, clics, retours à l'expéditeur, réclamations, rejets et échecs de rendu.	Amazon CloudWatch ou Amazon Data Firehose, ou par notification Amazon SNS, voir. Surveillance de l'envoi d'e-mails à l'aide de la publication d'événements (Des frais supplémentaires s'appliquent, voir Prix par métrique pour CloudWatch.)	Détails sur chaque événement	Précise (en fonction des caractéristiques de messagerie définies par l'utilisateur)
Publication d'événements en utilisant des domaines personnalisés associés à des jeux de configuration – Plus d'informations	Suivi des ouvertures et des clics.	Amazon CloudWatch ou Amazon Data Firehose, ou par notification Amazon SNS. (Des frais supplémentaires s'appliquent, voir Prix par métrique pour CloudWatch.)	Détails sur chaque événement.	Précise (en fonction des caractéristiques de messagerie définies par l'utilisateur)

> **Note**
>
> Il est possible que les métriques mesurées par les événements d'envoi d'e-mails ne respectent pas parfaitement vos quotas d'envoi. Cette différence peut être causée par les retours à l'expéditeur et les rejets d'e-mail, ou par l'utilisation du simulateur de boîte de réception Amazon SES. Pour connaître la marge de manœuvre que vous avez par rapport à vos quotas d'envoi, consultez Surveillance de vos quotas d'envoi.

Pour en savoir plus sur l'utilisation de chaque méthode de surveillance, consultez les rubriques suivantes :

- Surveillance de vos statistiques d'envoi à l'aide de la console Amazon SES
- Surveillance de vos statistiques d'utilisation à l'aide de l'API Amazon SES
- Surveillance de l'envoi d'e-mails à l'aide de la publication d'événements Amazon SES

Surveillance de vos statistiques d'envoi à l'aide de la console Amazon SES

À partir des pages Tableau de bord du compte, Métriques de réputation et Paramètres SMTP de la console Amazon SES, vous pouvez surveiller tous les envois d'e-mails, l'utilisation, les statistiques, les paramètres SMTP, l'état général de votre compte et les métriques de réputation. Les sections suivantes décrivent les métriques et les statistiques fournies sur chacune de ces pages de la console.

Il convient de noter que si les deux pages the section called “Tableau de bord du compte” et the section called “Métriques de réputation” de la console contiennent des métriques de retours à l'expéditeur et de réclamations, il existe une différence subtile entre ces deux ensembles de taux de retours à l'expéditeur et de réclamations, comme expliqué ci-dessous :

- Page Account dashboard (Tableau de bord du compte) — selon la plage de dates sélectionnée, vous pouvez voir quels étaient les taux de rebonds et de réclamations par le passé, ce qui indique la progression du changement des métriques jusqu'au moment présent.
- Page Reputation metrics (Métriques de réputation) : taux de retours à l'expéditeur et de réclamations basés sur le dernier point de données reçu lors du calcul de votre moyenne historique globale à un niveau élevé (cela ne doit pas être confondu avec votre taux de retours à l'expéditeur/réclamations régulier, qui correspond à des événements précis de retours à

l'expéditeur/réclamations tels qu'ils se produisent en temps réel, comme indiqué sur la page Account dashboard (Tableau de bord du compte).

Comme exemple simple pour comparer les taux de retours à l'expéditeur ou de réclamations entre la page Reputation metrics (Métriques de réputation) et la page Account dashboard (Tableau de bord du compte), supposons que le taux était de 2 % hier et qu'il est désormais de 1 %. Sur la page Account dashboard (Tableau de bord du compte), les graphiques vont tracer la progression graphique montrant un taux de 2 % pour hier et de 1 % pour aujourd'hui.

Tableau de bord du compte

Vous pouvez surveiller le nombre d'e-mails envoyés depuis votre compte, mais aussi le pourcentage de votre quota d'envoi qui a été utilisé, directement depuis la page Account dashboard (Tableau de bord du compte) de la console SES, dans le volet Daily email usage (Utilisation quotidienne des e-mails). Les taux de remise et de rejet correspondant à votre compte peuvent être contrôlés dans le volet Sending Statistics (Statistiques d'envoi), ainsi que d'autres facteurs clés liés à l'envoi de vos e-mails dans les volets suivants :

- Limites d'envoi – Contient les quotas suivants applicables à l'envoi de courrier via SES :
  - Daily sending quota (Quota d'envoi quotidien) : nombre maximal d'e-mails que vous pouvez envoyer sur une période de 24 heures.
  - Maximum send rate (Taux d'envoi maximum) : nombre maximal d'e-mails par seconde pouvant être envoyés à partir de votre compte.
- État du compte – Statut de votre compte SES :
  - `Healthy` – Aucun problème lié à la réputation n'affecte actuellement votre compte.
  - `Under review` – Des problèmes potentiels ont été identifiés avec votre compte SES - votre compte est en cours de révision pendant que vous travaillez à corriger les problèmes.
  - `Paused` – La capacité de votre compte à envoyer des e-mails est actuellement suspendue en raison d'un problème avec l'e-mail envoyé depuis votre compte. Lorsque le problème a été corrigé, vous pouvez demander que la capacité de votre compte à envoyer des e-mails soit reprise.
- Utilisation quotidienne des e-mails – Pour vérifier votre utilisation quotidienne afin de vous assurer que vous n'approchez pas de vos limites d'envoi :
  - Emails sent (E-mails envoyés) : nombre total d'e-mails envoyés sur une période de 24 heures.

  - Remaining sends (Envois restants) : nombre total d'e-mails restants disponibles sur une période de 24 heures.
  - Sending quota used (Quota d'envoi utilisé) : pourcentage de votre quota d'envoi quotidien utilisé.
- Sending Statistics (Statistiques d'envoi) – Xomprend des graphiques qui illustrent montrent la progression de quatre métriques clés dans un ensemble chronologique de points de données représentant les valeurs d'un type d'événement surveillé produisant des statistiques pour la plage de dates sélectionnée en utilisant une période d'agrégation d'1 heure. Vous pouvez sélectionner une plage de données avec des valeurs de départ de `Last 1 day` à `Last 14 days` pour filtrer les graphiques ci-dessous :
  - Sends (Envois) : somme des demandes d'envoi d'e-mails réussies.
  - Rejects (Rejets) : taux moyen de demandes d'envoi rejetées par SES basé sur `Rejects/Sends * 100` pour la plage de dates sélectionnée.
  - Bounces (Retours à l'expéditeur) : taux moyen dérivé de vos statistiques historiques de réputation globale d'expéditeur montrant la progression de la plage de dates sélectionnée.
  - Complaints (Plaintes) : taux moyen dérivé de vos statistiques historiques de réputation globale d'expéditeur montrant la progression de la plage de dates sélectionnée.

Chacun de ces graphiques comprend un bouton View in CloudWatch (Afficher dans CloudWatch), qui ouvre la métrique correspondante dans la console Amazon CloudWatch, permettant ainsi de consulter le détail des données, d'effectuer des calculs de métriques personnalisés et de créer des alarmes dans CloudWatch.

Métriques de réputation

Outre les taux de retours à l'expéditeur et de réclamations tels que discutés, la page Reputation metrics (Métriques de réputation) offre également une visibilité de haut niveau sur les facteurs clés affectant votre réputation.

- Summary (Récapitulatif) – Fournit une vue d'ensemble de l'état de votre réputation.
  - Status (Statut) : état global de la réputation basé sur les taux de retours à l'expéditeur et de plaintes historiques :
    - `Healthy` – Les deux métriques se trouvent à des niveaux normaux.
    - `Under review` – L'une ou les deux métriques ont automatiquement entraîné le placement sous vérification de votre compte.

    - `At risk` – L'une des métriques ou les deux ont atteint des niveaux inquiétants et la capacité de votre compte à envoyer des e-mails peut être menacée.
  - E-mails envoyés (dernières 24 heures) : nombre total d'e-mails envoyés sur les dernières 24 heures.
  - Envois restants : nombre total d'e-mails restants disponibles à envoyer sur une période de 24 heures.
  - Quota d'envoi utilisé : pourcentage de votre quota d'envoi quotidien utilisé.
- Contenu de l'onglet au niveau du compte :
  - Bounce rate (Taux de retours à l'expéditeur)
    - Status (Statut) : indique l'état de santé de votre taux de retours à l'expéditeur en utilisant les mêmes valeurs que celles décrites dans le volet de récapitulatif.
    - Historic bounce rate (Taux de retours à l'expéditeur historique) : pourcentage d'e-mails provenant de votre compte qui ont entraîné un retour à l'expéditeur fort calculé à partir de votre moyenne historique globale en fonction d'un volume représentatif qui représente vos pratiques d'envoi habituelles.
  - Complaint rate (Taux de réclamations)
    - Status (Statut) : indique l'état de santé de votre taux de réclamation en utilisant les mêmes valeurs que celles décrites dans le volet Résumé.
    - Historic bounce rate (Taux de retours à l'expéditeur historiques) : pourcentage d'e-mails envoyés depuis votre compte et signalés en tant que courrier indésirable par les destinataires et signalés en tant que courrier indésirable par les destinataires.
- Contenu de l'onglet Configuration set (Jeu de configurations) :
  - Réputation par jeu de configurations
    - Configuration set (Jeu de configurations) : permet de taper ou de sélectionner un jeu de configurations dont les métriques de réputation sont activées afin que vous puissiez voir les données de synthèse, de retour à l'expéditeur et de réclamation basées sur les e-mails envoyés à l'aide du jeu de configurations sélectionné. Les volets qui apparaissent après la sélection d'un jeu de configurations sont les mêmes que ceux décrits ci-dessus pour la page des métriques de réputation, sauf s'ils sont basés uniquement sur les e-mails envoyés avec le jeu de configurations sélectionné par rapport aux métriques d'envoi globales au niveau de votre compte.

Paramètres SMTP

Cette page répertorie les paramètres SMTP requis pour utiliser l'interface SMTP Amazon SES via l'API SES ou par programmation, et fournit des liens pour créer et gérer vos informations d'identification SMTP :

- Paramètres SMTP – Si vous souhaitez utiliser un langage de programmation, un serveur de messagerie ou une application compatible avec SMTP pour vous connecter à l'interface SMTP Amazon SES, les informations suivantes sont fournies :
  - Point de terminaison d'un SMTP
  - Port STARTTLS
  - protocole TLS (Transport Layer Security)
  - Port TLS Wrapper
  - Liens d'authentification fournis pour la création et la gestion des informations d'identification SMTP et IAM

Utilisation de la console pour la surveillance des métriques d'envoi et de réputation

Les procédures suivantes vous permettront de commencer à explorer vos mesures d'envoi et de réputation, soit à l'aide de la page Account dashboard (Tableau de bord du compte) pour les métriques basées sur l'historique récent (jusqu'à 14 jours), soit en utilisant la page Reputation metrics (Métriques de réputation) basées sur votre historique global jusqu'à présent.

Pour afficher les e-mails envoyés et les quotas d'envoi utilisés

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation, choisissez Account dashboard (Tableau de bord du compte). Vos statistiques d'utilisation figurent dans la section Daily email usage (Utilisation quotidienne des e-mails).

Pour afficher le nombre d'envois, les taux de rejets, de rebonds et de réclamations

1. Dans le panneau de navigation, choisissez Account dashboard (Tableau de bord du compte).

2. Dans Sending Statistics (Statistiques d'envoi), utilisez la liste déroulante Date range (Plage de dates) pour sélectionner la valeur de départ d'une plage de dates afin de filtrer les quatre graphiques situés directement en dessous de la section Sending Statistics (Statistiques d'envoi).
3. Selon la plage de dates sélectionnée, vous pouvez voir quels étaient les nombres et les taux par le passé, ce qui indique la progression du changement des métriques jusqu'au moment présent.
4. Dans chacun des graphiques, utilisez le bouton View in CloudWatch (Afficher dans CloudWatch) pour ouvrir la métrique correspondante dans la console Amazon CloudWatch, où vous pouvez consulter des données détaillées, effectuer des calculs de métriques personnalisés et créer des alarmes de surveillance dans CloudWatch.

Pour voir les taux historiques globaux de retours à l'expéditeur et de réclamations

1. Dans le panneau de navigation de gauche, choisissez Reputation metrics (Métriques de réputation).
2. Dans Bounce rate (Taux de retours à l'expéditeur), vous pouvez consulter le pourcentage d'e-mails envoyés depuis votre compte ayant entraîné un message d'erreur, et dans le Complaint rate (Taux de réclamations), vous pouvez consulter le pourcentage d'e-mails envoyés depuis votre compte et signalés en tant que courrier indésirable par les destinataires. Les deux métriques sont calculées à partir d'un volume représentatif d'e-mails basés sur vos pratiques d'envoi habituelles.
3. Dans chacun des panneaux, utilisez le bouton View in CloudWatch (Afficher dans CloudWatch) pour ouvrir la métrique correspondante dans la console Amazon CloudWatch, où vous pouvez consulter des données détaillées, effectuer des calculs de métriques personnalisés et créer des alarmes de surveillance dans CloudWatch.

Pour afficher les métriques de réputation par jeux de configurations

1. Dans le panneau de navigation de gauche, choisissez Reputation metrics (Métriques de réputation).
2. Sur la page des métriques de réputation, sélectionnez l'option Configuration set (Jeu de configurations).
3. Dans Reputation by configuration set (Réputation par jeu de configurations), cliquez dans le champ Configuration set (Jeu de configurations) et commencez à taper ou sélectionnez un jeu de configurations dont les métriques de réputation sont activées.

4. Une fois que vous avez sélectionné le jeu de configurations, les volets du récapitulatif, des retours à l'expéditeur et des réclamations sont chargés avec des métriques basées uniquement sur les e-mails envoyés avec le jeu de configurations sélectionné.

Surveillance de vos statistiques d'utilisation à l'aide de l'API Amazon SES

L'API Amazon SES fournit l'opération `GetSendStatistics`, qui renvoie des informations sur votre utilisation des services. Nous vous recommandons de vérifier vos statistiques d'envoi régulièrement, afin de pouvoir procéder à des ajustements si nécessaire.

Lorsque vous appelez l'opération `GetSendStatistics`, vous recevez une liste des points de données représentant les deux dernières semaines de votre activité d'envoi. Chaque point de données de cette liste représente 15 minutes d'activité et contient les informations suivantes pour cette période :

- Le nombre de messages d'erreur définitifs
- Le nombre de réclamations
- Le nombre de tentatives de remise (correspond au nombre d'e-mails envoyés)
- Le nombre de tentatives d'envoi rejetées
- Un horodatage pour la période d'analyse

Pour une description complète de l'opération `GetSendStatistics`, consultez le document Amazon Simple Email Service API Reference.

Dans cette section, vous allez retrouver les rubriques suivantes :

- the section called “Appel de l'opération d'API `GetSendStatistics` à l'aide de l'AWS CLI”
- the section called “Appel de l'opération `GetSendStatistics` par programmation”

Appel de l'opération d'API **`GetSendStatistics`** à l'aide de l'AWS CLI

La manière la plus simple d'appeler l'opération d'API `GetSendStatistics` consiste à utiliser l'AWS Command Line Interface (AWS CLI).

Pour appeler l'opération d'API **`GetSendStatistics`** à l'aide de l'AWS CLI

1. Si vous ne l'avez pas déjà fait, installez l AWS CLI.' Pour en savoir plus, consultez Installation de l'AWS Command Line Interface dans le Guide de l'utilisateur de l'AWS Command Line Interface.
2. Si vous ne l'avez pas déjà fait, configurez l'AWS CLI de manière à utiliser vos informations d'identification AWS. Pour en savoir plus, consultez « Configuration de l'AWS CLI » dans le Guide de l'utilisateur de l'AWS Command Line Interface.
3. Dans la ligne de commande, exécutez la commande suivante :

   ```
   aws ses get-send-statistics
   ```

   Si l'AWS CLI est configurée correctement, la liste des statistiques d'envoi au format JSON s'affiche. Chaque objet JSON inclut des statistiques d'envoi agrégées pour une période de 15 minutes.

Appel de l'opération **`GetSendStatistics`** par programmation

Vous pouvez également appeler l'opération `GetSendStatistics` par l'intermédiaire des kits SDK AWS. Cette section fournit des exemples de code pour les kits SDK AWS pour Go, PHP, Python et Ruby. Choisissez un des liens suivants pour afficher des exemples de code pour ce langage :

- Exemple de code pour le kit AWS SDK for Go
- Exemple de code pour le kit AWS SDK for PHP
- Exemple de code pour le kit AWS SDK for Python (Boto)
- Exemple de code pour le kit AWS SDK for Ruby

> **Note**
>
> Ces exemples de code supposent que vous avez créé un fichier d'informations d'identification partagé AWS qui contient votre ID de clé d'accès AWS, votre clé d'accès secrète AWS et votre région AWS préférée. Pour de plus amples informations, veuillez consulter Informations d'identification et fichiers de configuration partagés.

Appel de **`GetSendStatistics`** à l'aide du AWS SDK for Go

```
package main

import (
    "fmt"

    //go get github.com/aws/aws-sdk-go/...
    "github.com/aws/aws-sdk-go/aws"
    "github.com/aws/aws-sdk-go/aws/session"
    "github.com/aws/aws-sdk-go/service/ses"
    "github.com/aws/aws-sdk-go/aws/awserr"
)

const (
    // Replace us-west-2 with the AWS Region you're using for Amazon SES.
    AwsRegion = "us-west-2"
)

func main() {

    // Create a new session and specify an AWS Region.
    sess, err := session.NewSession(&aws.Config{
        Region:aws.String(AwsRegion)},
    )

    // Create an SES client in the session.
    svc := ses.New(sess)
    input := &ses.GetSendStatisticsInput{}

    result, err := svc.GetSendStatistics(input)

    // Display error messages if they occur.
    if err != nil {
        if aerr, ok := err.(awserr.Error); ok {
            switch aerr.Code() {
            default:
                fmt.Println(aerr.Error())
            }
        } else {
            // Print the error, cast err to awserr.Error to get the Code and
            // Message from an error.
            fmt.Println(err.Error())
```

```
        }
        return
    }

    fmt.Println(result)
}
```

Appel de **GetSendStatistics** à l'aide du AWS SDK for PHP

```
<?php

// Replace path_to_sdk_inclusion with the path to the SDK as described in
// http://docs.aws.amazon.com/aws-sdk-php/v3/guide/getting-started/basic-usage.html
define('REQUIRED_FILE','path_to_sdk_inclusion');

// Replace us-west-2 with the AWS Region you're using for Amazon SES.
define('REGION','us-west-2');

require REQUIRED_FILE;

use Aws\Ses\SesClient;

$client = SesClient::factory(array(
    'version'=> 'latest',
    'region' => REGION
));

try {
     $result = $client->getSendStatistics([]);
  echo($result);
} catch (Exception $e) {
     echo($e->getMessage()."\n");
}

?>
```

Appel de **GetSendStatistics** à l'aide du AWS SDK for Python (Boto)

```
import boto3 #pip install boto3
import json
from botocore.exceptions import ClientError
```

```
client = boto3.client('ses')

try:
    response = client.get_send_statistics(
)
except ClientError as e:
    print(e.response['Error']['Message'])
else:
    print(json.dumps(response, indent=4, sort_keys=True, default=str))
```

Appel de **`GetSendStatistics`** à l'aide du AWS SDK for Ruby

```
require 'aws-sdk' # gem install aws-sdk
require 'json'

# Replace us-west-2 with the AWS Region you're using for Amazon SES.
awsregion = "us-west-2"

# Create a new SES resource and specify a region
ses = Aws::SES::Client.new(region: awsregion)

begin

  resp = ses.get_send_statistics({
  })
  puts JSON.pretty_generate(resp.to_h)

# If something goes wrong, display an error message.
rescue Aws::SES::Errors::ServiceError => error
  puts error

end
```

Surveillance de l'envoi d'e-mails à l'aide de la publication d'événements Amazon SES

Pour vous permettre de suivre vos envois d'e-mails de manière détaillée, vous pouvez configurer Amazon SES pour publier les événements d'envoi d'e-mails sur Amazon CloudWatch, Amazon Data Firehose, Amazon Pinpoint ou Amazon Simple Notification Service en fonction des caractéristiques que vous définissez.

Vous pouvez suivre plusieurs types d'événements d'envoi d'e-mails, notamment les envois, les livraisons, les ouvertures, les clics, les rebonds, les réclamations, les refus, les échecs de rendu et les retards de livraison. Ces informations peuvent être utiles à des fins analytiques et opérationnelles. Par exemple, vous pouvez publier vos données d'envoi d'e-mails CloudWatch et créer des tableaux de bord qui suivent les performances de vos campagnes par e-mail, ou vous pouvez utiliser Amazon SNS pour vous envoyer des notifications lorsque certains événements se produisent.

Comment fonctionne la publication d'événements avec les ensembles de configuration et les balises de message

Pour utiliser la publication d'événements, vous devez commencer par configurer un ou plusieurs ensembles de configuration. Un jeu de configurations spécifie l'emplacement de publication des événements, ainsi que les types d'événements à publier. Ensuite, chaque fois que vous enverrez un e-mail, indiquez le nom du jeu de configurations, ainsi qu'une ou plusieurs balises de message sous forme de paires nom/valeur, afin de classer l'e-mail. Par exemple, si vous faites la promotion de livres, vous pouvez nommer une balise de message genre et attribuer la valeur sci-fi ou western lorsque vous envoyez un e-mail pour la campagne associée.

Selon l'interface d'envoi d'e-mail que vous utilisez, vous pouvez soit fournir la balise de message en tant que paramètre `EmailTags`dans le champ de l'opération d'`SendEmail`API, soit l'ajouter à l'en-tête de message spécifique à SES. `X-SES-MESSAGE-TAGS` Pour en savoir plus sur les jeux de configuration, consultez Utilisation des jeux de configuration dans Amazon SES.

Outre les balises de message que vous spécifiez, Amazon SES ajoute des balises automatiques aux messages que vous envoyez. Vous n'avez pas besoin d'effectuer des étapes supplémentaires pour utiliser des balises automatiques.

Le tableau suivant répertorie les balises automatique qui sont automatiquement appliquées aux messages que vous envoyez à l'aide d'Amazon SES.

Balises automatiques pour Amazon SES

Nom de balise automatique	Description
`ses:caller-identity`	Identité IAM de l'utilisateur Amazon SES qui a envoyé l'e-mail.
`ses:configuration-set`	Nom du jeu de configurations associé à l'e-mail.
`ses:from-domain`	Domaine de l'adresse de l'expéditeur.

Nom de balise automatique	Description
`ses:outgoing-ip`	Adresse IP qu' Amazon SES a utilisée pour envoyer l'e-mail.
`ses:source-ip`	Adresse IP que l'appelant a utilisée pour envoyer l'e-mail.
`ses:source-tls-version`	Version du protocole TLS que l'appelant a utilisée pour envoyer l'e-mail.

Feedback précis pour les campagnes par e-mail

La `ses:feedback-id-<a or b>` balise est une balise de message facultative que vous pouvez considérer comme une balise hybride ou semi-automatique. Bien qu'elle soit similaire aux balises automatiques décrites dans la section précédente, la différence est que vous devez l'ajouter manuellement et utiliser la clé de préfixe. `ses:` Vous pouvez utiliser jusqu'à deux de ces balises définies par `ses:feedback-id-a` et`ses:feedback-id-b`.

Lorsque vous spécifiez ces balises, SES les ajoute automatiquement à l'`Feedback-ID`en-tête standard qui est utilisé pour fournir des statistiques de livraison, telles que les taux de plaintes et de spam, dans le cadre d'une boucle de rétroaction (FBL), voir. Boucles de rétroaction L'`Feedback-ID`en-tête est composé de l'identifiant, SESInternalID, utilisé par SES pour collecter les informations relatives aux plaintes, et de la balise statique, AmazonSES, identifiant SES en tant que plateforme d'envoi, telle que :

`FeedBackId:feedback-id-a:feedback-id-b:((SESInternalID):(AmazonSES))`

Ces balises d'identification de commentaires facultatives vous permettent de générer des commentaires précis, par exemple pour les messages que vous envoyez dans le cadre d'une campagne par e-mail. Vous pouvez l'utiliser `ses:feedback-id-<a or b>` en le spécifiant sous forme de balise de message dans le `EmailTags`champ de la demande d'`SendEmail`opération, comme indiqué dans l'exemple suivant :

```
{
  "FromEmailAddress": "noreply@example.com",
  "Destination": {
    "ToAddresses": [
      "customer@example.net"
```

```
    ]
  },
  "Content": {
    "Simple": {
      "Subject": {
        "Data": "Hello and welcome"
      },
      "Body": {
        "Text": {
          "Data": "Lorem ipsum dolor sit amet."
        },
        "Html": {
          "Data": "Lorem ipsum dolor sit amet."
        }
      }
    }
  },
  "EmailTags": [
    {
      "Name": "ses:feedback-id-a",
      "Value": "new-members-campaign"
    },
    {
      "Name": "ses:feedback-id-b",
      "Value": "football-campaign"
    }
  ],
  "ConfigurationSetName": "football-club"
}
```

Si vous envoyez au format brut, vous devez l'ajouter `ses:feedback-id-<a or b>` en tant que balise de message à l'en-tête spécifique à SES. `X-SES-MESSAGE-TAGS`

La balise de `ses:feedback-id-<a or b>` message peut également être CloudWatch suivie sur Amazon en la spécifiant comme source de CloudWatch valeur, comme toute autre balise de message, voir the section called “Ajouter les détails de la destination de l' CloudWatch événement” (Des frais supplémentaires s'appliquent, voir Prix par métrique pour CloudWatch.)

Utilisation de la publication d'événements

Les sections suivantes contiennent les informations dont vous avez besoin pour configurer et utiliser la publication d'événements Amazon SES.

- Configuration de la publication d'événements
- Utilisation des données d'événement

Terminologie de publication d'événements

La liste suivante définit les termes liés à la publication d'événements Amazon SES.

Événement d'envoi d'e-mail

Les informations associées au résultat d'un e-mail que vous soumettez à Amazon SES. Les événements d'envoi incluent ce qui suit :

- Send (Envoi) – La demande d'envoi a réussi et Amazon SES tente de remettre le message au serveur de messagerie du destinataire. (Si une suppression globale ou au niveau du compte est utilisée, SES la comptera toujours comme un envoi, mais la livraison sera supprimée).
- RenderingFailure— L'e-mail n'a pas été envoyé en raison d'un problème de rendu du modèle. Ce type d'événement peut se produire lorsqu'il manque des données du modèle ou lorsqu'il n'y a pas concordance entre les paramètres du modèle et les données. Ce type d'événement ne se produit que lorsque vous envoyez un e-mail à l'aide des opérations d'API `SendTemplatedEmail` ou `SendBulkTemplatedEmail`.
- Reject (Rejet) – Amazon SES a accepté l'e-mail, a déterminé qu'il contenait un virus et l'a rejeté. Amazon SES n'a pas tenté de remettre l'e-mail au serveur de messagerie du destinataire.
- Delivery (Livraison) – Amazon SES a bien remis l'e-mail au serveur de messagerie du destinataire.
- Bounce – Message d'erreur définitif indiquant que le serveur de messagerie du destinataire a définitivement rejeté l'e-mail. Les soft bounces (messages d'erreur temporaires) sont inclus uniquement quand Amazon SES ne parvient pas à remettre l'e-mail après plusieurs tentatives au cours d'une période donnée.
- Complaint (Réclamation) – L'e-mail a été correctement remis au serveur de messagerie du destinataire, mais le destinataire l'a marqué comme courrier indésirable.
- DeliveryDelay— L'e-mail n'a pas pu être remis au serveur de messagerie du destinataire en raison d'un problème temporaire. Des retards de livraison peuvent se produire, par exemple lorsque la boîte de réception du destinataire est pleine ou lorsque le serveur de messagerie de réception rencontre un problème transitoire.

- Subscription (Abonnement) – L'e-mail a été envoyé avec succès, mais le destinataire a mis à jour les préférences d'abonnement en cliquant sur `List-Unsubscribe` dans l'en-tête de l'e-mail ou le lien `Unsubscribe` dans le pied-de-page.
- Open (Ouverture) – Le destinataire a reçu le message et l'a ouvert dans son client de messagerie.
- Click (Clic) – Le destinataire a cliqué sur un ou plusieurs liens contenus dans l'e-mail.

Jeu de configurations

Ensemble de règles définissant la destination vers laquelle Amazon SES publie les événements d'envoi d'e-mails et les types d'événements d'envoi d'e-mails que vous souhaitez publier. Lorsque vous envoyez un e-mail que vous voulez utiliser avec la publication d'événements, vous spécifiez le jeu de configurations à associer à l'e-mail.

Destination de l'événement

AWS Service sur lequel vous publiez des événements d'envoi d'e-mails Amazon SES. Chaque destination d'événement que vous configurez appartient à un, et à un seul, jeu de configurations.

Balise de message

Paire nom/valeur utilisée pour classer un e-mail à des fins de publication d'événements. Par exemple, campagne/livre et campagne/vêtements. Lorsque vous envoyez un e-mail, vous spécifiez la balise de message en tant que paramètre à l'appel d'API ou en tant qu'en-tête d'e-mail spécifique à Amazon SES.

Balise automatique

Balises de messages qui sont automatiquement incluses dans les rapports de publication d'événements. Il existe une balise automatique pour le nom du jeu de configuration, le domaine de l'adresse d'expédition, l'adresse IP sortante de l'appelant, l'adresse IP sortante Amazon SES et l'identité IAM de l'appelant.

Configuration de la publication d'événements Amazon SES

Cette section décrit la procédure à suivre pour configurer Amazon SES de façon à publier vos événements d'envoi d'e-mails aux services AWS suivants :

- Amazon CloudWatch
- Amazon Data Firehose
- Amazon Pinpoint

- Amazon Simple Notification Service (Amazon SNS)

Les étapes suivantes, nécessaires à la configuration de la publication d'événements, sont décrites dans les rubriques ci-dessous :

1. Vous devez créer un jeu de configurations à l'aide de la console ou de l'API Amazon SES.
2. Ajoutez une ou plusieurs destinations d'événements (FirehoseCloudWatch, Pinpoint ou SNS) à l'ensemble de configuration et configurez des paramètres propres à la destination de l'événement.
3. Lorsque vous envoyez un e-mail, vous devez spécifier le jeu de configuration à utiliser qui contient la destination de votre événement.

Rubriques de cette section

Étape 1 : Création d'un jeu de configurations

Vous devez d'abord disposer d'un jeu de configuration pour mettre en place la publication d'événements. Si vous n'avez pas encore de jeu de configuration, ou si vous souhaitez en créer un nouveau, consultez Création de jeux de configuration dans SES

Vous pouvez également créer des jeux de configuration à l'aide de l'opération CreateConfigurationSet dans l'API Amazon SES V2 ou l'Amazon SES CLI v2, voir Créer un jeu de configurations (AWS CLI).

Étape 2 : Ajout d'une destination d'événement

Les destinations d'événements sont des endroits où vous publiez des événements Amazon SES Chaque destination d'événement que vous configurez appartient à un, et à un seul, jeu de configurations. Lorsque vous configurez une destination d'événement avec Amazon SES, vous choisissez la destination du AWS service et vous spécifiez les paramètres associés à cette destination.

Lorsque vous configurez une destination d'événement, vous pouvez choisir d'envoyer des événements à l'un des AWS services suivants :

- Amazon CloudWatch
- Amazon Data Firehose
- Amazon EventBridge
- Amazon Pinpoint
- Amazon Simple Notification Service (Amazon SNS)

La destination d'événement que vous choisissez dépend du niveau de détail voulu sur les événements et de la façon dont vous souhaitez recevoir les informations sur les événements. Si vous voulez simplement un total cumulé pour chaque type d'événement (par exemple, afin de pouvoir définir une alarme lorsque le total devient trop élevé), vous pouvez utiliser CloudWatch.

Si vous souhaitez des enregistrements d'événements détaillés que vous pouvez envoyer à un autre service tel qu'Amazon OpenSearch Service ou Amazon Redshift à des fins d'analyse, vous pouvez utiliser Firehose.

Si vous souhaitez recevoir des notifications lorsque certains événements se produisent, choisissez Amazon SNS.

Cette section contient les rubriques suivantes :

- Configurer une destination d' CloudWatch événement pour la publication d'événements
- Configurer une destination d'événements Data Firehose pour la publication d'événements Amazon SES
- Configurer une EventBridge destination Amazon pour la publication d'événements
- Configuration d'une destination d'événement Amazon Pinpoint pour la publication d'événements
- Configurer une destination d'événement Amazon SNS pour la publication d'événements

Configurer une destination d' CloudWatch événement pour la publication d'événements

Avec Amazon CloudWatch Metrics, vous pouvez utiliser les destinations des événements pour publier les événements d'envoi d'e-mails vers Amazon SES CloudWatch. Comme une destination d' CloudWatch événement ne peut être configurée que dans un ensemble de configuration, vous devez d'abord créer un ensemble de configuration, puis ajouter la destination de l'événement au jeu de configuration.

Lorsque vous ajoutez une destination d' CloudWatch événement à un ensemble de configuration, vous devez choisir une ou plusieurs CloudWatch dimensions correspondant aux balises de message

que vous utilisez lorsque vous envoyez vos e-mails. À l'instar des balises de message, une CloudWatch dimension est une paire nom/valeur qui vous aide à identifier une métrique de manière unique.

Par exemple, vous pouvez utiliser une balise de message et une dimension appelée `campaign` pour identifier votre campagne d'e-mailing. Lorsque vous publiez vos événements d'envoi d'e-mails sur CloudWatch, il est important de choisir les balises et les dimensions de vos messages, car ces choix ont une incidence sur votre CloudWatch facturation et déterminent la manière dont vous pouvez filtrer les données de vos événements d'envoi d'e-mails CloudWatch.

Cette section fournit des informations pour vous aider à choisir vos dimensions, puis montre comment ajouter une destination d' CloudWatch événement à un ensemble de configuration.

Rubriques de cette section

- Ajout d'une destination d'événement CloudWatch
- Choix des CloudWatch dimensions

Ajout d'une destination d'événement CloudWatch

La procédure décrite dans cette section explique comment ajouter les détails de la destination d'un CloudWatch événement à un ensemble de configuration et suppose que vous avez effectué les étapes 1 à 6 dansCréation d'une destination d'événement.

Vous pouvez également utiliser l'opération UpdateConfigurationSetEventDestination dans l'API Amazon SES V2 pour créer et modifier les destinations des événements.

Pour ajouter les détails de la destination de l' CloudWatch événement à un ensemble de configuration à l'aide de la console

1. Voici les instructions détaillées pour sélectionner le type CloudWatch de destination de votre événement à l'étape 7 et en supposant que vous avez effectué toutes les étapes précédentesCréation d'une destination d'événement. Après avoir sélectionné le type de CloudWatch destination, saisi un nom de destination et activé la publication d'événements, le volet des CloudWatch dimensions Amazon s'affiche. Ses champs sont traités dans les étapes suivantes. (Des frais supplémentaires s'appliquent, voir Prix par métrique pour CloudWatch.)
2. Pour Value Source, spécifiez comment Amazon SES obtiendra les données auxquelles elles seront transmises CloudWatch. Les sources de valeur suivantes sont disponibles :

- Message Tag (Balise de message) – Amazon SES extrait le nom et la valeur de la dimension d'une balise que vous spécifiez à l'aide de l'en-tête `X-SES-MESSAGE-TAGS` ou du paramètre d'API `EmailTags`. Pour en savoir plus sur l'utilisation des balises de message, consultez la page the section called “Étape 3 : Spécifier votre jeu de configurations lors de l'envoi”.

  > **Note**
  >
  > Les balises de messages peuvent inclure les chiffres de 0 à 9, les lettres A-Z (majuscules et minuscules), des tirets (-) et des traits de soulignement (_).

  Vous pouvez également utiliser la source de valeur Message Tag (Balise de message) pour créer des dimensions en fonction des balises automatiques pour Amazon SES. Pour utiliser une balise automatique, tapez le nom de cette balise automatique en tant que Dimension Name (Nom de la dimension). Par exemple, pour créer une dimension basée sur la balise automatique de jeu de configurations, utilisez `ses:configuration-set` pour Dimension Name (Nom de la dimension), et le nom du jeu de configurations pour Default Value (Valeur par défaut). Pour obtenir la liste complète des balises automatiques, consultez Comment fonctionne la publication d'événements avec les ensembles de configuration et les balises de message.
- Email Header (En-tête d'e-mail) – Amazon SES extrait le nom et la valeur de la dimension d'un en-tête dans l'e-mail.

  > **Note**
  >
  > Vous ne pouvez pas utiliser les en-têtes d'e-mail suivants comme Dimension Name (Nom de dimension) : `Received`, `To`, `From`, `DKIM-Signature`, `CC`, `message-id` ou `Return-Path`.

- Link Tag (Balise de lien) – Amazon SES extrait le nom et la valeur de la dimension d'une balise que vous avez spécifiée dans un lien. Pour en savoir plus sur l'ajout des balises, consultez Puis-je baliser les liens avec des identificateurs uniques ?.

3. Dans Nom de la dimension, tapez le nom de la dimension à laquelle vous souhaitez passer CloudWatch.

> **Note**
>
> Les noms de dimension peuvent uniquement contenir des lettres ASCII (a à z, A à Z), des chiffres (0 à 9), des traits de soulignement (_) ou des tirets (-). Les espaces, les caractères accentués, les caractères non latins et les autres caractères spéciaux ne sont pas autorisés.

4. Dans Default Value (Valeur par défaut), saisissez la valeur de la dimension.

> **Note**
>
> Les valeurs de dimension ne peuvent contenir que des lettres ASCII (a à z, A à Z), des chiffres (0 à 9), des traits de soulignement (_), des tirets (-), des signes (@) et des points (.). Les espaces, les caractères accentués, les caractères non latins et les autres caractères spéciaux ne sont pas autorisés.

5. Pour ajouter d'autres dimensions, sélectionnez Add Dimension (Ajouter une dimension). Sinon, choisissez Next (Suivant).
6. Sur l'écran de révision, si vous êtes satisfait de la façon dont vous avez défini votre destination d'événement, choisissez Add destination (Ajouter une destination).

Choix des CloudWatch dimensions

Lorsque vous choisissez des noms et des valeurs à utiliser comme CloudWatch dimensions, tenez compte des facteurs suivants :

- Prix par métrique — Vous pouvez consulter les statistiques de base d'Amazon SES CloudWatch gratuitement. Toutefois, lorsque vous collectez des statistiques à l'aide de la publication d'événements, vous encourez des coûts de surveillance CloudWatch détaillée. Chaque combinaison unique de type d'événement, de nom de dimension et de valeur de dimension crée une métrique différente dans CloudWatch. Lorsque vous utilisez CloudWatch la surveillance détaillée, vous êtes facturé pour chaque métrique. Pour cette raison, vous pouvez décider de ne pas choisir de dimensions qui peuvent prendre de nombreuses valeurs différentes. Par exemple, à moins que vous soyez très intéressé par le suivi de vos événements d'envoi d'e-mails par domaine d'expédition, vous pouvez décider de ne pas définir de dimension pour la balise automatique `ses:from-domain` Amazon SES, car elle peut prendre de nombreuses valeurs différentes. Pour plus d'informations, consultez Tarification d'CloudWatch.

- Filtrage des métriques : si une métrique possède plusieurs dimensions, vous ne pouvez pas accéder à la métrique en CloudWatch fonction de chaque dimension séparément. Pour cette raison, réfléchissez bien avant d'ajouter plusieurs dimensions à une même destination d' CloudWatch événement. Par exemple, si vous souhaitez des métriques par `campaign` et par combinaison de `campaign` et `genre`, vous devez ajouter deux destinations d'événement : l'une avec uniquement `campaign` comme dimension, et l'autre avec `campaign` et `genre` comme dimensions.
- Source des valeurs de dimension – Au lieu de spécifier vos valeurs de dimension en utilisant des en-têtes propres à Amazon SES ou un paramètre destiné à l'API, vous pouvez également choisir de laisser Amazon SES prendre les valeurs de dimension de vos propres en-têtes de message MIME. Vous pouvez opter pour cette solution si vous utilisez déjà des en-têtes personnalisés et que vous ne voulez pas modifier vos e-mails ou vos appels à l'API d'envoi d'e-mails de façon à collecter les métriques en fonction de vos valeurs d'en-tête. Si vous utilisez vos propres en-têtes de message MIME pour la publication d'événements Amazon SES, les noms et les valeurs d'en-tête que vous utilisez pour la publication d'événements Amazon SES peuvent uniquement inclure les lettres A à Z, les nombres 0 à 9, les traits de soulignement (_), les arobas (@), les traits d'union (-) et les points (.). Si vous spécifiez un nom ou une valeur contenant d'autres caractères, l'appel d'envoi d'e-mail réussira toujours, mais les statistiques de l'événement ne seront pas envoyées à Amazon CloudWatch.

Pour plus d'informations sur CloudWatch les concepts, consultez Amazon CloudWatch Concepts dans le guide de CloudWatch l'utilisateur Amazon.

Configurer une destination d'événements Data Firehose pour la publication d'événements Amazon SES

Une destination d'événement Amazon Data Firehose représente une entité qui publie des événements spécifiques d'envoi d'e-mails Amazon SES vers Firehose. Comme la destination d'un événement Firehose ne peut être configurée que dans un ensemble de configuration, vous devez d'abord créer un ensemble de configuration. Ensuite, vous ajoutez la destination de l'événement au jeu de configuration.

La procédure décrite dans cette section explique comment ajouter les détails de la destination des événements Firehose à un ensemble de configuration et suppose que vous avez effectué les étapes 1 à 6 dans. Création d'une destination d'événement

Vous pouvez également utiliser l'opération UpdateConfigurationSetEventDestination dans la destination Amazon SES API V2 pour créer et mettre à jour les destinations des événements.

Pour ajouter les détails de la destination des événements Firehose à un ensemble de configuration à l'aide de la console

1. Voici les instructions détaillées pour sélectionner Firehose comme type de destination d'événement à l'étape 7 et en supposant que vous avez effectué toutes les étapes précédentes. Création d'une destination d'événement Après avoir sélectionné le type de destination Firehose, saisi un nom de destination et activé la publication d'événements, le volet du flux de diffusion Amazon Data Firehose s'affiche. Ses champs sont traités dans les étapes suivantes.
2. Pour le flux de diffusion, choisissez un flux de diffusion Firehose existant ou choisissez Create new stream pour en créer un nouveau à l'aide de la console Firehose.

   Pour plus d'informations sur la création d'un flux à l'aide de la console Firehose, consultez la section Création d'un flux de diffusion Amazon Kinesis Firehose dans le manuel Amazon Data Firehose Developer Guide.
3. Pour le rôle Identity and Access Management (IAM), choisissez un rôle IAM pour lequel Amazon SES est autorisé à publier sur Firehose en votre nom. Vous pouvez choisir un rôle existant, demander à Amazon SES de créer un rôle à votre place ou créer votre propre rôle.

   Si vous choisissez un rôle existant ou si vous créez votre propre rôle, vous devez modifier manuellement les politiques du rôle pour autoriser le rôle à accéder au flux de diffusion Firehose et pour autoriser Amazon SES à assumer ce rôle. Pour obtenir des exemples de politiques, consultez Autoriser Amazon SES à publier sur votre flux de diffusion Firehose.
4. Choisissez Next (Suivant).
5. Sur l'écran de révision, si vous êtes satisfait de la façon dont vous avez défini votre destination d'événement, choisissez Add destination (Ajouter une destination).

Pour plus d'informations sur l'utilisation de l'`UpdateConfigurationSetEventDestination`API pour ajouter une destination d'événement Firehose, consultez le manuel Amazon Simple Email Service API Reference.

Autoriser Amazon SES à publier sur votre flux de diffusion Firehose

Pour permettre à Amazon SES de publier des enregistrements dans votre flux de diffusion Firehose, vous devez utiliser un rôle AWS Identity and Access Management (IAM) et associer ou modifier la politique d'autorisation et la politique de confiance du rôle. La politique d'autorisations permet au rôle de publier des enregistrements sur votre flux de diffusion Firehose, et la politique de confiance permet à Amazon SES d'assumer ce rôle.

Cette section fournit des exemples des deux stratégies. Pour obtenir des informations sur l'attachement de stratégies à des rôles IAM, consultez Modification d'un rôle dans le Guide de l'utilisateur IAM.

stratégie d'autorisations

La politique d'autorisation suivante permet au rôle de publier des enregistrements de données dans votre flux de diffusion Firehose.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Action": [
        "firehose:PutRecordBatch"
      ],
      "Resource": [
        "arn:aws:firehose:delivery-region:111122223333:deliverystream/delivery-stream-name"
      ]
    }
  ]
}
```

Dans l'exemple précédent, apportez les modifications suivantes :

- Remplacez *la région de livraison* par la AWS région dans laquelle vous avez créé le flux de diffusion Firehose.
- Remplacez *111122223333* par votre ID de compte AWS .
- Remplacez *delivery-stream-name par le nom* du flux de diffusion Firehose.

Stratégie d’approbation

La stratégie d'approbation suivante permet à Amazon SES d'assumer ce rôle.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ses.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "111122223333",
          "AWS:SourceArn": "arn:aws:ses:delivery-region:111122223333:configuration-
set/configuration-set-name"
        }
      }
    }
  ]
}
```

Dans l'exemple précédent, apportez les modifications suivantes :

- Remplacez *la région de livraison* par la AWS région dans laquelle vous avez créé le flux de diffusion Firehose.
- Remplacez *111122223333* par votre ID de compte AWS .
- Remplacez *configuration-set-name* par le nom de votre ensemble de configuration associé au flux de diffusion Firehose.

Configurer une EventBridge destination Amazon pour la publication d'événements

Une destination d' EventBridge événement Amazon vous informe des événements d'envoi d'e-mails que vous spécifiez dans un ensemble de configuration. SES génère et envoie des événements d'envoi d'e-mails au bus d'événements EventBridge par défaut. Un bus d'événements est un routeur qui reçoit des événements et peut les transmettre à plusieurs destinations. Vous pouvez en savoir plus sur l'intégration des événements d'envoi d'e-mails EventBridge à Amazon dansSurveillance à l'aide EventBridge. Comme une destination d' EventBridge événement ne peut être configurée que dans un ensemble de configuration, vous devez créer un ensemble de configuration avant d'ajouter la destination de l'événement au jeu de configuration.

La procédure décrite dans cette section explique comment ajouter les détails de la destination d'un EventBridge événement à un ensemble de configuration et suppose que vous avez effectué les étapes 1 à 6 dansCréation d'une destination d'événement.

Vous pouvez également utiliser l'opération UpdateConfigurationSetEventDestination dans l'API Amazon SES V2 pour créer et modifier les destinations des événements.

Pour ajouter les détails de la destination de l' EventBridge événement à un ensemble de configuration à l'aide de la console

1. Voici les instructions détaillées pour sélectionner le type EventBridge de destination de votre événement à l'étape 7 et en supposant que vous avez effectué toutes les étapes précédentesCréation d'une destination d'événement. Après avoir sélectionné le type de EventBridge destination Amazon, saisi un nom de destination et activé la publication d'événements, un volet d'information sur le bus d' EventBridge événements Amazon s'affiche.
2. Choisissez Next (Suivant).
3. Sur l'écran de révision, si vous êtes satisfait de la façon dont vous avez défini votre destination d'événement, choisissez Add destination (Ajouter une destination). La page de résumé de la destination de l'événement s'ouvrira et une bannière de réussite confirmera que la destination de l'événement a été créée ou modifiée avec succès.

Configuration d'une destination d'événement Amazon Pinpoint pour la publication d'événements

La destination d'un événement Amazon Pinpoint vous informe des événements d'envoi d'e-mails que vous spécifiez dans un ensemble de configuration. Comme la destination d'un événement Amazon Pinpoint ne peut être configurée que dans un ensemble de configuration, vous devez créer un ensemble de configuration avant d'ajouter la destination de l'événement au jeu de configuration.

La procédure de cette section montre comment ajouter les détails de la destination d'événement Amazon Pinpoint à un jeu de configurations et suppose que vous avez effectué les étapes 1 à 6 de la procédure de Création d'une destination d'événement.

Vous pouvez également utiliser l'opération UpdateConfigurationSetEventDestination dans l'API Amazon SES V2 pour créer et modifier les destinations des événements.

Des frais supplémentaires s'appliquent pour les types de canaux que vous avez configurés dans vos projets Amazon Pinpoint. Pour plus d'informations, veuillez consulter Tarification d'Amazon Pinpoint.

Pour ajouter les détails d'une destination d'événement Amazon Pinpoint à un jeu de configurations à l'aide de la console

1. Voici les instructions détaillées pour sélectionner Amazon Pinpoint comme type de destination d'événement à l'étape 7. Cela suppose que vous avez terminé toutes les étapes précédentes de la procédure de Création d'une destination d'événement.

   > **Note**
   >
   > Amazon Pinpoint ne prend pas en charge les types d'événements Retards de livraison ou Abonnements.

   Après avoir sélectionné le type de destination Amazon Pinpoint, saisi un nom de destination et activé la publication d'événements, le volet des détails du projet Amazon Pinpoint s'affiche. Ses champs sont traités dans les étapes suivantes.

2. Pour Projet, choisissez un projet Amazon Pinpoint existant ou choisissez Create a new project in Amazon Pinpoint (Créer un projet dans Amazon Pinpoint) pour en créer un nouveau.

   Pour plus d'informations sur la création d'un projet, consultez Create a project (Création d'un projet) dans le manuel Amazon Pinpoint User Guide.

3. Choisissez Next (Suivant).

4. Sur l'écran de révision, si vous êtes satisfait de la façon dont vous avez défini votre destination d'événement, choisissez Add destination (Ajouter une destination). La page de résumé de la destination de l'événement s'ouvrira et une bannière de réussite confirmera que la destination de l'événement a été créée ou modifiée avec succès.

Configurer une destination d'événement Amazon SNS pour la publication d'événements

La destination d'un événement Amazon SNS vous informe des événements d'envoi d'e-mails que vous spécifiez dans un ensemble de configuration. Comme la destination d'un événement Amazon SNS ne peut être configurée que dans un ensemble de configuration, vous devez créer un ensemble de configuration avant d'ajouter la destination de l'événement au jeu de configuration.

La procédure de cette section montre comment ajouter les détails de la destination des événements Amazon SNS à un jeu de configuration et suppose que vous avez effectué les étapes 1 à 6 dans Création d'une destination d'événement.

Vous pouvez également utiliser l'opération UpdateConfigurationSetEventDestination dans l'API Amazon SES V2 pour créer et modifier les destinations des événements.

> **Note**
>
> Les notifications de commentaires concernant les retours à l'expéditeur, les réclamations et les livraisons peuvent également être configurées via Amazon SNS pour n'importe laquelle de vos identités d'expéditeur vérifiées. Pour plus d'informations, consultez the section called "Configuration des notifications Amazon SNS".

Il y a des frais supplémentaires pour l'envoi de messages aux points de terminaison abonnés à vos rubriques Amazon SNS. Pour plus d'informations, consultez la tarification Amazon SNS.

Pour ajouter les détails d'une destination Amazon SNS à un jeu de configurations à l'aide de la console

1. Voici les instructions détaillées pour sélectionner Amazon SNS comme type de destination d'événement dans Étape 7. Cela suppose que vous avez terminé toutes les étapes précédentes de Création d'une destination d'événement. Après avoir sélectionné le type de destination Amazon SNS, saisi un nom de destination et activé la publication d'événements, le volet thématique Amazon Simple Notification Service (SNS) s'affiche. Ses champs sont traités dans les étapes suivantes.
2. Pour Topic SNS (Rubrique SNS), choisissez une rubrique Amazon SNS existante ou choisissez Create new topic SNS (Créer une rubrique SNS) pour en créer une nouvelle.

   Pour en savoir plus, consultez Création d'une rubrique (Create a Topic) dans le Guide du développeur d'Amazon Simple Notification Service .

   > **Important**
   >
   > Lorsque vous créez votre rubrique à l'aide d'Amazon SNS, pour Type, choisissez uniquement Standard. (SES ne prend pas en charge les rubriques de type FIFO.)

3. Choisissez Next (Suivant).
4. Sur l'écran de révision, si vous êtes satisfait de la façon dont vous avez défini votre destination d'événement, choisissez Add destination (Ajouter une destination). La page de résumé de la

destination de l'événement s'ouvrira et une bannière de réussite confirmera que la destination de l'événement a été créée ou modifiée avec succès.

5. Que vous créiez une nouvelle rubrique SNS ou sélectionniez une rubrique existante, vous devez donner un accès à SES pour publier des notifications sur la rubrique. Sur la page récapitulative de la destination de l'événement à partir de l'étape précédente, choisissez Amazon SNS à partir de la colonne Destination type (Type de destination), cela vous mènera à la list Topics (Rubriques) dans la console Amazon Simple Notification Service, effectuez les étapes suivantes à partir de la console Amazon SNS :

   a. Sélectionnez le nom de la rubrique SNS que vous avez créée ou modifiée à l'étape précédente.

   b. Sur l'écran de détails du sujet, choisissez Edit (Modifier).

   c. Pour donner à Amazon SES la permission de publier des notifications sur la rubrique, sur l'écran Edit topic (Modifier la rubrique) de la console SNS, développez Access policy (Stratégie d'accès) et dans JSON editor (Éditeur JSON), ajoutez la politique d'autorisation suivante :

```
{
  "Version": "2012-10-17",
  "Id": "notification-policy",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ses.amazonaws.com"
      },
      "Action": "sns:Publish",
      "Resource": "arn:aws:sns:topic_region:111122223333:topic_name",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "111122223333",
          "AWS:SourceArn":
 "arn:aws:ses:topic_region:111122223333:configuration-set/configuration-set-
name"
        }
      }
    }
  ]
}
```

Dans l'exemple précédent, apportez les modifications suivantes :

- Remplacez *topic_region* par la région AWS dans laquelle vous avez créé la rubrique SNS.
- Remplacez *111122223333* par votre identifiant de compte. AWS
- Remplacez *topic_name* par le nom de votre rubrique SNS.
- Remplacez *configuration-set-name* par le nom de votre jeu de configuration associé à la destination de l'événement SNS.

d. Sélectionnez Enregistrer les modifications.

Étape 3 : Spécifier votre jeu de configuration lorsque vous envoyez un e-mail

Une fois que vous avez créé un jeu de configurations et ajouté une destination d'événement, la dernière étape de la publication d'événements consiste à envoyer vos e-mails.

Pour publier les événements associés à un e-mail, vous devez indiquer le nom du jeu de configurations à associer à l'e-mail. Vous pouvez éventuellement fournir des balises de message pour classer l'e-mail dans une catégorie.

Vous fournissez ces informations à Amazon SES sous forme de paramètres pour l'API d'envoi d'e-mails, d'en-têtes d'e-mail propres à ou d'en-têtes personnalisés dans votre message MIME. La méthode que vous choisissez dépend de l'interface d'envoi d'e-mails que vous utilisez, comme le montre le tableau suivant.

Interface d'envoi d'e-mails	Méthodes de publication d'événements
`SendEmail`	Paramètres d'API
`SendTemplatedEmail`	Paramètres d'API
`SendBulkTemplatedEmail`	Paramètres d'API
`SendCustomVerificationEmail`	Paramètres d'API
`SendRawEmail`	Paramètres d'API, en-têtes d'e-mail propres à Amazon SES ou en-têtes MIME personnalisés

Interface d'envoi d'e-mails	Méthodes de publication d'événements
	Important Si vous spécifiez des balises de message en utilisant à la fois des en-têtes de message et des paramètres d'API, Amazon SES utilise uniquement les balises de message fournies par les paramètres d'API. Amazon SES ne joint pas les balises de message spécifiées par les paramètres d'API et les en-têtes.
Interface SMTP	En-têtes d'e-mail propres à Amazon SES

Les sections suivantes expliquent comment spécifier le jeu de configurations et les balises de message à l'aide d'en-têtes et de paramètres d'API.

- Utilisation des paramètres d'API Amazon SES
- Utilisation d'en-têtes d'e-mail propres à Amazon SES
- Utilisation d'en-têtes d'e-mail personnalisés

Note

Vous pouvez éventuellement inclure des balises de message dans les en-têtes de vos e-mails. Les balises de messages peuvent inclure les chiffres de 0 à 9, les lettres A-Z (majuscules et minuscules), des tirets (-) et des traits de soulignement (_).

Utilisation des paramètres d'API Amazon SES

Pour utiliser SendEmail, SendTemplatedEmail, SendBulkTemplatedEmail, SendCustomVerificationEmail ou SendRawEmail dans le cadre de la publication d'événements, vous devez spécifier le jeu de configurations et les identifications de message en transmettant les structures de données appelées ConfigurationSet et MessageTag à l'appel d'API.

Pour en savoir plus sur l'utilisation de l'API Amazon SES, consultez le document Amazon Simple Email Service API Reference.

Utilisation d'en-têtes d'e-mail propres à Amazon SES

Lorsque vous utilisez `SendRawEmail` ou l'interface SMTP, vous pouvez spécifier le jeu de configurations et les balises de message en ajoutant à l'e-mail des en-têtes propres à Amazon SES. Amazon SES supprime les en-têtes avant d'envoyer l'e-mail. Le tableau suivant présente les noms des en-têtes à utiliser.

Informations de publication d'événements	En-tête
Jeu de configurations	`X-SES-CONFIGURATION-SET`
Balises de message	`X-SES-MESSAGE-TAGS`

L'exemple suivant montre l'aspect des têtes dans un e-mail brut que vous envoyez à Amazon SES.

```
X-SES-MESSAGE-TAGS: tagName1=tagValue1, tagName2=tagValue2
X-SES-CONFIGURATION-SET: myConfigurationSet
From: sender@example.com
To: recipient@example.com
Subject: Subject
Content-Type: multipart/alternative;
 boundary="----=_boundary"

------=_boundary
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit

body
------=_boundary
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 7bit

body
------=_boundary--
```

Utilisation d'en-têtes d'e-mail personnalisés

Bien que vous soyez tenu de spécifier le nom du jeu de configurations à l'aide de l'en-tête propre à Amazon SES `X-SES-CONFIGURATION-SET`, vous pouvez spécifier les message des balises en utilisant vos propres en-têtes MIME.

> **Note**
>
> Les noms et les valeurs d'en-tête que vous utilisez pour la publication d'événements Amazon SES doivent être en ASCII. Si vous spécifiez un nom ou une valeur d'en-tête non ASCII pour la publication d'événements Amazon SES, l'appel d'envoi d'e-mails continue d'aboutir, mais les métriques d'événement ne sont pas émises vers Amazon CloudWatch.

Utilisation des données d'événement Amazon SES

Une fois que vous avez configuré la publication de l'événement et spécifié un jeu de configurations pour envoyer des e-mails, vous pouvez récupérer vos événements d'envoi d'e-mail à partir de l'événement de destination que vous avez spécifié lors de la configuration du jeu de configurations associé à l'e-mail.

Cette section explique comment récupérer vos événements d'envoi d'e-mails depuis Amazon CloudWatch et Amazon Data Firehose, et comment interpréter les données d'événements fournies par Amazon SNS.

- Récupération de données d'événements Amazon SES à partir de CloudWatch
- Récupération des données d'événements Amazon SES depuis Firehose
- Interprétation des données d'événement Amazon SES à partir d'Amazon SNS

Récupération de données d'événements Amazon SES à partir de CloudWatch

Amazon SES peut publier les métriques de vos événements d'envoi d'e-mails dans Amazon CloudWatch. Lorsque vous publiez les données d'événements sur CloudWatch, il fournit ces métriques comme ensemble ordonné de données chronologiques. Vous pouvez utiliser ces métriques pour surveiller les performances de votre envoi d'e-mails. Par exemple, vous pouvez surveiller la métrique de réclamation et définir une alarme CloudWatch à déclencher lorsque la métrique dépasse une valeur donnée.

Il existe deux niveaux de granularité auxquels Amazon SES peut publier ces événements dans CloudWatch :

- Sur votre compte Compte AWS – Ces métriques, qui correspondent aux mesures que vous surveillez à l'aide de la console Amazon SES et de l'API `GetSendStatistics`, sont disponibles sur l'ensemble de votre Compte AWS. Amazon SES publie automatiquement ces métriques dans CloudWatch.
- Fine-grained (Détaillées) – Ces métriques sont classées par caractéristiques d'e-mail que vous définissez à l'aide des balises de message. Pour publier ces métriques dans CloudWatch, vous devez configurer la publication d'événements à l'aide d'une destination d'événement CloudWatch et spécifier un jeu de configurations lorsque vous envoyez un e-mail. Vous pouvez également spécifier des balises de message ou utiliser des balises automatiques qu'Amazon SES fournit automatiquement.

Cette section décrit les métriques disponibles et comment afficher les métriques dans CloudWatch.

Métriques disponibles

Vous pouvez publier les métriques suivantes d'envoi d'e-mail Amazon SES sur CloudWatch :

- Send (Envoi) – La demande d'envoi a réussi et Amazon SES tente de remettre le message au serveur de messagerie du destinataire. (Si une suppression globale ou au niveau du compte est utilisée, SES la comptera toujours comme un envoi, mais la livraison sera supprimée).
- RenderingFailure – L'e-mail n'a pas été envoyé en raison d'un problème de rendu du modèle. Ce type d'événement peut se produire lorsqu'il manque des données du modèle ou lorsqu'il n'y a pas concordance entre les paramètres du modèle et les données. Ce type d'événement ne se produit que lorsque vous envoyez un e-mail à l'aide des opérations d'API `SendTemplatedEmail` ou `SendBulkTemplatedEmail`.
- Reject (Rejet) – Amazon SES a accepté l'e-mail, a déterminé qu'il contenait un virus et l'a rejeté. Amazon SES n'a pas tenté de remettre l'e-mail au serveur de messagerie du destinataire.
- Delivery (Livraison) – Amazon SES a bien remis l'e-mail au serveur de messagerie du destinataire.
- Bounce – Message d'erreur définitif indiquant que le serveur de messagerie du destinataire a définitivement rejeté l'e-mail. Les soft bounces (messages d'erreur temporaires) sont inclus uniquement quand Amazon SES ne parvient pas à remettre l'e-mail après plusieurs tentatives au cours d'une période donnée.
- Complaint (Réclamation) – L'e-mail a été correctement remis au serveur de messagerie du destinataire, mais le destinataire l'a marqué comme courrier indésirable.

- DeliveryDelay – L'e-mail n'a pas pu être remis au serveur de messagerie du destinataire, car un problème temporaire s'est produit. Des retards de livraison peuvent se produire, par exemple lorsque la boîte de réception du destinataire est pleine ou lorsque le serveur de messagerie de réception rencontre un problème transitoire.
- Subscription (Abonnement) – L'e-mail a été envoyé avec succès, mais le destinataire a mis à jour les préférences d'abonnement en cliquant sur `List-Unsubscribe` dans l'en-tête de l'e-mail ou le lien `Unsubscribe` dans le pied-de-page.
- Open (Ouverture) – Le destinataire a reçu le message et l'a ouvert dans son client de messagerie.
- Click (Clic) – Le destinataire a cliqué sur un ou plusieurs liens contenus dans l'e-mail.

Dimensions disponibles

CloudWatch utilise les noms de dimension que vous spécifiez lorsque vous ajoutez une destination d'événement CloudWatch à une configuration définie dans Amazon SES. Pour plus d'informations, consultez Configurer une destination d' CloudWatch événement pour la publication d'événements.

Affichage des métriques Amazon SES dans la console CloudWatch

La procédure suivante décrit comment afficher vos métriques de publication d'événements Amazon SES à l'aide de la console CloudWatch.

Pour afficher les métriques à l'aide de la console CloudWatch

1. Connectez-vous à la AWS Management Console et ouvrez la console CloudWatch à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Si nécessaire, changez la région. Dans la barre de navigation, sélectionnez la région où résident vos ressources AWS. Pour en savoir plus, consultez Régions et points de terminaison.
3. Dans le volet de navigation, sélectionnez Toutes les métriques.
4. Dans le volet Métriques, sélectionnez SES.
5. Sélectionnez la métrique que vous voulez afficher. Pour consulter les métriques de publication d'événement détaillées, choisissez la combinaison de dimensions que vous avez spécifiée lors de la configuration de votre destination d'événement CloudWatch. Pour en savoir plus sur l'affichage des métriques avec CloudWatch, consultez Utiliser les métriques Amazon CloudWatch.

Pour afficher les métriques à l'aide de la AWS CLI

- À partir d'une invite de commande, utilisez la commande suivante :

```
aws cloudwatch list-metrics --namespace "AWS/SES"
```

Récupération des données d'événements Amazon SES depuis Firehose

Amazon SES publie les événements d'envoi d'e-mails à Firehose sous forme d'enregistrements JSON. Firehose publie ensuite les enregistrements vers la destination du AWS service que vous avez choisie lorsque vous avez configuré le flux de diffusion dans Firehose. Pour plus d'informations sur la configuration des flux de diffusion Firehose, consultez la section Création d'un flux de diffusion Firehose dans le manuel Amazon Data Firehose Developer Guide.

Rubriques de cette section :

- Contenu des données d'événements publiées par Amazon SES sur Firehose
- Exemples de données d'événements publiées par Amazon SES sur Firehose

Contenu des données d'événements publiées par Amazon SES sur Firehose

Amazon SES publie des enregistrements d'événements d'envoi d'e-mails à Amazon Data Firehose au format JSON. Lors de la publication d'événements sur Firehose, Amazon SES suit chaque enregistrement JSON avec un caractère de nouvelle ligne.

Vous pouvez trouver des exemples de registres pour tous ces types de notifications dans Exemples de données d'événements publiées par Amazon SES sur Firehose.

Rubriques de cette section

- Objet JSON de niveau supérieur
- Objet de l'e-mail
- Objet bounce
- Objet de réclamation
- Objet Delivery
- Objet Send
- Objet Reject

- Objet Open
- Objet Click
- Objet Rendering Failure
- DeliveryDelay objet
- Objet Abonnement

Objet JSON de niveau supérieur

L'objet JSON de niveau supérieur d'un registre d'événement d'envoi d'e-mail contient les champs suivants.

Nom de champ	Description
`eventType`	Chaîne qui décrit le type d'événement. Valeurs possibles : `Bounce`, `Complaint` , `Delivery`, `Send`, `Reject`, `Open`, `Click`, `Rendering Failure`, `DeliveryDelay` ou `Subscription` . Si vous n'avez pas effectué la Configuration de la publication d'événements, ce champ est nommé `notificationType` .
`mail`	Objet JSON qui contient des informations sur l'e-mail qui a généré l'événement.
`bounce`	Ce champ est présent uniquement si `eventType` a la valeur `Bounce`. Il contient des informations sur le retour à l'expéditeur.
`complaint`	Ce champ est présent uniquement si `eventType` a la valeur `Complaint` . Il contient des informations sur la réclamation.
`delivery`	Ce champ est présent uniquement si `eventType` a la valeur `Delivery`. Il contient des informations sur la remise.

Nom de champ	Description
`send`	Ce champ est présent uniquement si `eventType` a la valeur `Send`.
`reject`	Ce champ est présent uniquement si `eventType` a la valeur `Reject`. Il contient des informations sur le rejet.
`open`	Ce champ est présent uniquement si `eventType` a la valeur `Open`. Il contient des informations sur l'événement ouvert.
`click`	Ce champ est présent uniquement si `eventType` a la valeur `Click`. Il contient des informations sur l'événement de clic.
`failure`	Ce champ est présent uniquement si `eventType` a la valeur `Rendering Failure`. Il contient des informations sur l'événement d'échec d'affichage.
`deliveryDelay`	Ce champ est présent uniquement si `eventType` a la valeur `DeliveryDelay`. Il contient des informations sur la livraison différée d'un e-mail.
`subscription`	Ce champ est présent uniquement si `eventType` a la valeur `Subscription`. Il contient des informations sur les préférences d'abonnement.

Objet de l'e-mail

Chaque registre d'événement d'envoi d'e-mail contient des informations sur l'e-mail d'origine dans l'objet `mail`. L'objet JSON qui contient les informations sur un objet `mail` comporte les champs suivants.

Nom de champ	Description
`timestamp`	Date et heure au format ISO8601 (AAAA-MM-JJThh:mm:ss.sZ) auxquelles le message a été envoyé.
`messageId`	ID unique attribué par Amazon SES au message. Amazon SES vous a renvoyé cette valeur lorsque vous avez envoyé le message. **Note** Cet ID de message a été attribué par Amazon SES. Vous trouverez l'ID de message de l'e-mail d'origine dans les champs `headers` et `commonHeaders` de l'objet `mail`.
`source`	Adresse e-mail à partir de laquelle le message a été envoyé (adresse MAIL FROM de l'enveloppe).
`sourceArn`	ARN (Amazon Resource Name) de l'identité qui a été utilisée pour envoyer l'e-mail. Dans le cas d'une autorisation d'envoi, `sourceArn` correspond à l'ARN de l'identité dont le propriétaire a autorisé l'utilisation pour l'envoi de l'e-mail par l'expéditeur délégué. Pour en savoir plus sur l'autorisation d'envoi, consultez Méthodes d'authentification d'e-mail.
`sendingAccountId`	ID de compte AWS du compte utilisé pour envoyer l'e-mail. Dans le cas de l'autorisation d'envoi, `sendingAccountId` correspond à l'ID de compte de l'expéditeur délégué.

Nom de champ	Description
`destination`	Liste des adresses e-mail destinataires de l'e-mail original.
`headersTruncated`	Chaîne qui spécifie si les en-têtes ont été tronqués dans la notification, ce qui a lieu s'ils ont une taille supérieure à 10 Ko. Les valeurs possibles sont `true` et `false`.
`headers`	Liste des en-têtes d'origine de l'e-mail. Chaque en-tête de la liste a un champ `name` et un champ `value`. **Note** Tout ID de message du champ `headers` provient du message d'origine que vous avez transmis à Amazon SES. L'ID de message qu'Amazon SES a ensuite affecté au message se trouve dans le champ `messageId` de l'objet `mail`.
`commonHeaders`	Mappage des en-têtes originaux de l'e-mail communément utilisés. **Note** Tout ID de message contenu dans le champ `commonHeaders` correspond à l'ID de message qu'Amazon SES a par la suite affecté au message dans le champ `messageId` de l'objet `mail`.
`tags`	Une liste des identifications associées à l'e-mail.

Objet bounce

L'objet JSON qui contient les informations sur un événement `Bounce` comporte toujours les champs suivants.

Nom de champ	Description
`bounceType`	Type de retour à l'expéditeur, tel que déterminé par Amazon SES.
`bounceSubType`	Sous-type de retour à l'expéditeur, tel que déterminé par Amazon SES.
`bouncedRecipients`	Liste qui contient les informations sur les destinataires de l'e-mail d'origine ayant fait l'objet d'un retour à l'expéditeur.
`timestamp`	Date et heure au format ISO8601 (AAAA-MM-JJThh:mm:ss.sZ) auxquelles l'ISP a envoyé la notification de retour à l'expéditeur.
`feedbackId`	ID unique du retour à l'expéditeur.
`reportingMTA`	Valeur du champ `Reporting-MTA` du DSN. Il s'agit de la valeur de la MTA qui a tenté d'effectuer l'opération de remise, de relais ou de passerelle décrite dans le DSN. **Note** Ce champ n'apparaît que si une notification de statut de livraison (DSN) a été attachée au retour à l'expéditeur.

Destinataires à l'origine d'un retour à l'expéditeur

Un événement de retour à l'expéditeur peut se rapporter à un seul destinataire ou à plusieurs destinataires. Le champ `bouncedRecipients` contient une liste d'objets (un objet par destinataire auquel l'événement de retour à l'expéditeur s'applique), ainsi que le champ suivant.

Nom de champ	Description
`emailAddress`	Adresse e-mail du destinataire. Si un DSN est disponible, l'adresse correspond à la valeur du champ `Final-Recipient` du DSN.

En outre, si un DSN est attaché au retour à l'expéditeur, les champs suivants peuvent également être présents.

Nom de champ	Description
`action`	Valeur du champ `Action` du DSN. Cette valeur indique l'action effectuée par la MTA de suivi comme résultat de sa tentative de remettre le message à ce destinataire.
`status`	Valeur du champ `Status` du DSN. Il s'agit du code de statut indépendant du transport par destinataire qui indique le statut de remise du message.
`diagnosticCode`	Code de statut émis par la MTA de suivi. Il s'agit de la valeur du champ `Diagnostic-Code` du DSN. Ce champ peut être absent du DSN (et donc également absent du JSON).

Types de retour à l'expéditeur

Chaque évènement de retour à l'expéditeur présente l'un des types affichés dans le tableau suivant.

Le système de publication d'événements ne publie que les retours à l'expéditeur définitifs ou temporaires qui ne seront plus réessayés par Amazon SES. Lorsque vous recevez des retours à l'expéditeur marqués `Permanent`, vous devez supprimer les adresses e-mail correspondantes de votre liste de diffusion ; vous ne pourrez plus leur envoyer d'e-mails à l'avenir. Des retours à l'expéditeur `Transient` vous sont envoyés lorsqu'un message a fait plusieurs fois l'objet d'un message d'erreur temporaire, et qu'Amazon SES a arrêté toute tentative de remise. Plus tard, vous aurez peut-être la possibilité de renvoyer avec succès l'e-mail à une adresse ayant dans un premier temps généré un retour à l'expéditeur `Transient`.

bounceType	bounceSubType	Description
`Undetermined`	`Undetermined`	Amazon SES n'a pas pu déterminer de motif de retour à l'expéditeur.
`Permanent`	`General`	Amazon SES a reçu un message d'erreur définitif général. Si vous recevez ce type de retour à l'expéditeur, vous devez supprimer l'adresse e-mail du destinataire de votre liste de diffusion.
`Permanent`	`NoEmail`	Amazon SES a reçu un message d'erreur définitif, car l'adresse e-mail cible n'existe pas. Si vous recevez ce type de retour à l'expédit eur, vous devez supprimer l'adresse e-mail du destinataire de votre liste de diffusion.
`Permanent`	`Suppressed`	Amazon SES a supprimé l'envoi à cette adresse, car elle a un historique récent de retour à l'expéditeur sous la forme d'adresse non valide. Pour remplacer la liste de suppressi on globale, consultez Utilisation de la liste de suppression au niveau du compte Amazon SES.
`Permanent`	`OnAccountSuppressi onList`	Amazon SES a supprimé l'envoi à cette adresse car celle-ci figure dans la liste de suppression au niveau du compte. Cela n'est

bounceType	bounceSubType	Description
		pas pris en compte dans votre métrique de taux de retours à l'expéditeur.
`Transient`	`General`	Amazon SES a reçu un retour à l'expéditeur général. Vous pouvez réessayer avec succès l'envoi à ce destinataire à l'avenir.
`Transient`	`MailboxFull`	Amazon SES a reçu un retour à l'expéditeur de boîte aux lettres pleine. Vous pouvez réessayer avec succès l'envoi à ce destinataire à l'avenir.
`Transient`	`MessageTooLarge`	Amazon SES a reçu un message de retour à l'expéditeur trop volumineux. Vous pouvez réessayer avec succès l'envoi à ce destinataire si vous réduisez la taille du message.
`Transient`	`ContentRejected`	Amazon SES a reçu un retour à l'expéditeur de contenu rejeté. Vous pouvez réessayer avec succès l'envoi à ce destinataire si vous modifiez le contenu du message.
`Transient`	`AttachmentRejected`	Amazon SES a reçu un retour à l'expéditeur de pièce jointe rejetée. Vous pouvez réessayer avec succès l'envoi à ce destinataire si vous supprimez ou modifiez la pièce jointe.

Objet de réclamation

L'objet JSON qui contient les informations sur un événement `Complaint` comporte les champs suivants.

Nom de champ	Description
`complainedRecipients`	Liste contenant des informations sur les destinataires qui ont soumis la réclamation.

Nom de champ	Description
`timestamp`	Date et heure au format ISO8601 (AAAA-MM-JJThh:mm:ss.sZ) auxquelles l'ISP a envoyé la notification de réclamation.
`feedbackId`	ID unique de la réclamation.
`complaintSubType`	Sous-type de la réclamation, tel que déterminé par Amazon SES.

De plus, si un rapport de commentaire est attaché à la réclamation, les champs suivants peuvent être présents.

Nom de champ	Description
`userAgent`	Valeur du champ `User-Agent` du rapport de commentaires. Cette valeur indique le nom et la version du système ayant généré le rapport.
`complaintFeedbackType`	Valeur du champ `Feedback-Type` du rapport de commentaires reçu de l'ISP. La valeur contient le type de commentaires.
`arrivalDate`	Valeur du champ `Arrival-Date` ou `Received-Date` du rapport de commentaires au format ISO8601 (YYYY-MM-DDThh:mm:ss.sZ). Le champ peut être absent du rapport (et donc également absent du JSON).

Destinataires à l'origine d'une réclamation

Le champ `complainedRecipients` contient la liste des destinataires susceptibles d'avoir déposé la réclamation.

> **Important**
>
> Comme la plupart des FAI rédigent l'adresse e-mail du destinataire à l'origine de la réclamation à partir de la notification de réclamation, cette liste contient les informations sur les destinataires susceptibles d'avoir envoyé la réclamation, basées sur les destinataires du message d'origine et sur le FAI à partir duquel la réclamation a été reçue. Amazon SES effectue une recherche sur le message d'origine afin de déterminer la liste des destinataires.

Les objets JSON de cette liste contiennent le champ suivant.

Nom de champ	Description
`emailAddress`	Adresse e-mail du destinataire.

Types de réclamation

Vous pouvez voir les types de réclamation suivants dans le champ `complaintFeedbackType` tels qu'attribués par l'ISP du rapport, selon le site web IANA (Internet Assigned Numbers) :

Nom de champ	Description
`abuse`	Indique un e-mail indésirable ou un autre type d'e-mail malveillant.
`auth-failure`	Rapport d'échec d'authentification d'e-mail.
`fraud`	Indique certains types de fraude ou d'activité d'hameçonnage.
`not-spam`	Indique que l'entité qui fournit le rapport ne considère pas le message en tant que courrier indésirable. Cette option permet de corriger un message qui a été mal balisé ou classé à tort comme courrier indésirable.
`other`	Indique tout autre commentaire ne pouvant être classé dans les autres types enregistrés.

Nom de champ	Description
`virus`	Signale qu'un virus a été détecté dans le message d'origine.

Objet Delivery

L'objet JSON qui contient les informations sur un événement `Delivery` comporte toujours les champs suivants.

Nom de champ	Description
`timestamp`	Date et heure auxquelles Amazon SES a remis l'e-mail au serveur de messagerie du destinataire, au format ISO8601 (AAAA-MM-JJThh:mm:ss.sZ).
`processingTimeMillis`	Délai, en millisecondes, entre le moment où Amazon SES a accepté la demande de l'expéditeur et le moment où Amazon SES a transmis le message au serveur de messagerie du destinataire.
`recipients`	Liste des destinataires auxquels l'événement de remise s'applique.
`smtpResponse`	Message de réponse SMTP du FAI distant ayant accepté l'e-mail depuis Amazon SES. Ce message varie selon l'e-mail, le serveur de messagerie de réception et l'ISP de réception.
`reportingMTA`	Nom d'hôte du serveur de messagerie Amazon SES ayant envoyé l'e-mail.

Objet Send

L'objet JSON qui contient les informations sur un événement `send` est toujours vide.

Objet Reject

L'objet JSON qui contient les informations sur un événement `Reject` comporte toujours les champs suivants.

Nom de champ	Description
`reason`	Raison du rejet de l'e-mail. La seule valeur possible est `Bad content`, ce qui signifie qu'Amazon SES a détecté que l'e-mail contenait un virus. Lorsqu'un message est rejeté, Amazon SES arrête de le traiter et ne tente pas de le remettre au serveur de messagerie du destinataire.

Objet Open

L'objet JSON qui contient les informations sur un événement `Open` comporte toujours les champs suivants.

Nom de champ	Description
`ipAddress`	Adresse IP du destinataire.
`timestamp`	Date et heure auxquelles l'événement open s'est produit, au format ISO8601 (AAAA-MM-JJThh:mm:ss.sZ).
`userAgent`	Agent utilisateur de l'appareil ou client de messagerie que le destinataire a utilisé pour ouvrir l'e-mail.

Objet Click

L'objet JSON qui contient les informations sur un événement `Click` comporte toujours les champs suivants.

Nom de champ	Description
`ipAddress`	Adresse IP du destinataire.
`timestamp`	Date et heure auxquelles l'événement de clic s'est produit, au format ISO8601 (AAAA-MM-JJThh:mm:ss.sZ).
`userAgent`	Agent utilisateur du client que le destinataire a utilisé pour cliquer sur un lien dans l'e-mail.
`link`	URL du lien sur lequel le destinataire a cliqué.
`linkTags`	Liste des balises ajoutées au lien à l'aide de l'attribut `ses:tags`. Pour en savoir plus sur l'ajout de balises aux liens de vos e-mails, consultez Q5. Puis-je baliser les liens avec des identificateurs uniques ? dans le FAQ sur les métriques Amazon SES d'envoi d'e-mails.

Objet Rendering Failure

L'objet JSON qui contient les informations sur un événement `Rendering Failure` comporte les champs suivants.

Nom de champ	Description
`templateName`	Nom du modèle utilisé pour envoyer l'e-mail.
`errorMessage`	Message qui fournit des informations supplémentaires sur l'échec d'affichage.

DeliveryDelay objet

L'objet JSON qui contient les informations sur un événement `DeliveryDelay` comporte les champs suivants.

Nom de champ	Description
`delayType`	Type de retard. Les valeurs possibles sont : • InternalFailure— Un problème interne à Amazon SES a retardé le message. • General – Une défaillance générique s'est produite au cours de la conversation SMTP. • MailboxFull— La boîte aux lettres du destinataire est pleine et ne peut pas recevoir de messages supplémentaires. • SpamDetected— Le serveur de messageri e du destinataire a détecté un grand nombre d'e-mails non sollicités provenant de votre compte. • RecipientServerError— Un problème temporaire avec le serveur de messageri e du destinataire empêche la livraison du message. • IPFailure – L'adresse IP qui envoie le message est bloquée ou réduite par le fournisseur de messagerie du destinataire. • TransientCommunicationFailure— Un échec de communication temporaire s'est produit lors de la conversation SMTP avec le fournisseur de messagerie du destinataire. • BYOIP HostNameLookupUnavailable — Amazon SES n'a pas pu rechercher le nom d'hôte DNS de vos adresses IP. Ce type de délai ne se produit que lorsque vous utilisez Bring Your Own IP (Fourniture de vos propres adresses IP). • Undetermined – Amazon SES n'a pas été en mesure de déterminer la raison du retard de livraison.

Nom de champ	Description
	• SendingDeferral— Amazon SES a jugé approprié de reporter le message en interne.
`delayedRecipients`	Objet contenant des informations sur le destinataire de l'e-mail.
`expirationTime`	Date et heure auxquelles Amazon SES cessera d'essayer de remettre le message. Cette valeur est affichée au format ISO 8601.
`reportingMTA`	Adresse IP de l'agent de transfert de messages (MTA) qui a signalé le retard.
`timestamp`	La date et l'heure auxquelles le retard s'est produit, illustrées au format ISO 8601.

Destinataires retardés

L'objet `delayedRecipients` contient les valeurs suivantes.

Nom de champ	Description
`emailAddress`	Adresse électronique ayant entraîné un retard dans la livraison du message.
`status`	Code d'état SMTP associé au délai de livraison.
`diagnosticCode`	Code de diagnostic fourni par l'agent de transfert de message (MTA) récepteur.

Objet Abonnement

L'objet JSON qui contient les informations sur un événement `Subscription` comporte les champs suivants.

Nom de champ	Description
`contactList`	Nom de la liste sur laquelle figure le contact.
`timestamp`	Date et heure au format ISO8601 (AAAA-MM-JJThh:mm:ss.sZ) auxquelles l'ISP a envoyé la notification de retour à l'expéditeur.
`source`	Adresse e-mail à partir de laquelle le message a été envoyé (adresse MAIL FROM de l'enveloppe).
`newTopicPreferences`	Structure de données JSON (carte) qui spécifie l'état d'abonnement de toutes les rubriques de la liste de contacts en indiquant le statut après une modification (contact abonné ou désabonné).
`oldTopicPreferences`	Structure de données JSON (carte) qui spécifie le statut d'abonnement de toutes les rubriques de la liste de contacts en indiquant l'état avant la modification (contact souscrit ou désabonné).

Préférences de la nouvelle ou de l'ancienne rubrique

Les objets `newTopicPreferences` et `oldTopicPreferences` contiennent les valeurs suivantes.

Nom de champ	Description
`unsubscribeAll`	Indique si le contact s'est désabonné de toutes les rubriques de la liste de contacts.
`topicSubscriptionStatus`	Spécifie le sujet dans le `topicName` champ et mappe le statut de l'abonnement (OptInou OptOut) dans le `subscriptionStatus` champ.

Nom de champ	Description
`topicDefaultSubscriptionStatus`	Spécifie le sujet dans le `topicName` champ et mappe le statut de l'abonnement (OptInou OptOut) dans le `subscriptionStatus` champ.

Exemples de données d'événements publiées par Amazon SES sur Firehose

Cette section fournit des exemples des types d'enregistrements d'événements d'envoi d'e-mails publiés par Amazon SES sur Firehose.

Rubriques de cette section :

- registre de retour à l'expéditeur
- registre de réclamation
- registre de remise
- registre d'envoi
- registre de rejet
- registre d'ouverture
- registre de clic
- registre d'échec de rendu
- DeliveryDelay record
- Abonnement

> **Note**
>
> Dans les exemples suivants, où un champ `tag` est utilisé, il utilise la publication d'événements via un jeu de configuration pour lequel SES prend en charge la publication d'étiquettes pour tous les types d'événements. Si vous utilisez des notifications de commentaires directement sur l'identité, SES ne publie pas d'étiquettes. Découvrez comment ajouter des étiquettes lors de la création d'un jeu de configuration ou de la modification d'un jeu de configuration.

registre de retour à l'expéditeur

Voici un exemple d'enregistrement d'`Bounce`événement publié par Amazon SES sur Firehose.


```
{
  "eventType":"Bounce",
  "bounce":{
    "bounceType":"Permanent",
    "bounceSubType":"General",
    "bouncedRecipients":[
      {
        "emailAddress":"recipient@example.com",
        "action":"failed",
        "status":"5.1.1",
        "diagnosticCode":"smtp; 550 5.1.1 user unknown"
      }
    ],
    "timestamp":"2017-08-05T00:41:02.669Z",
    "feedbackId":"01000157c44f053b-61b59c11-9236-11e6-8f96-7be8aexample-000000",
    "reportingMTA":"dsn; mta.example.com"
  },
  "mail":{
    "timestamp":"2017-08-05T00:40:02.012Z",
    "source":"Sender Name <sender@example.com>",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "headers":[
      {
        "name":"From",
        "value":"Sender Name <sender@example.com>"
      },
      {
        "name":"To",
        "value":"recipient@example.com"
      },
      {
        "name":"Subject",
        "value":"Message sent from Amazon SES"
      },
```

```
      {
        "name":"MIME-Version",
        "value":"1.0"
      },
      {
        "name":"Content-Type",
        "value":"multipart/alternative; boundary=\"----
=_Part_7307378_1629847660.1516840721503\""
      }
    ],
    "commonHeaders":{
      "from":[
        "Sender Name <sender@example.com>"
      ],
      "to":[
        "recipient@example.com"
      ],
      "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject":"Message sent from Amazon SES"
    },
    "tags":{
      "ses:configuration-set":[
        "ConfigSet"
      ],
      "ses:source-ip":[
        "192.0.2.0"
      ],
      "ses:from-domain":[
        "example.com"
      ],
      "ses:caller-identity":[
        "ses_user"
      ]
    }
  }
}
```

registre de réclamation

Voici un exemple d'enregistrement d'`Complaint`événement publié par Amazon SES sur Firehose.

```
{
  "eventType":"Complaint",
  "complaint": {
```

```
    "complainedRecipients":[
      {
        "emailAddress":"recipient@example.com"
      }
    ],
    "timestamp":"2017-08-05T00:41:02.669Z",
    "feedbackId":"01000157c44f053b-61b59c11-9236-11e6-8f96-7be8aexample-000000",
    "userAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/60.0.3112.90 Safari/537.36",
    "complaintFeedbackType":"abuse",
    "arrivalDate":"2017-08-05T00:41:02.669Z"
  },
  "mail":{
    "timestamp":"2017-08-05T00:40:01.123Z",
    "source":"Sender Name <sender@example.com>",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "headers":[
      {
        "name":"From",
        "value":"Sender Name <sender@example.com>"
      },
      {
        "name":"To",
        "value":"recipient@example.com"
      },
      {
        "name":"Subject",
        "value":"Message sent from Amazon SES"
      },
      {
        "name":"MIME-Version","value":"1.0"
      },
      {
        "name":"Content-Type",
        "value":"multipart/alternative; boundary=\"----
=_Part_7298998_679725522.1516840859643\""
      }
    ],
```

```
    "commonHeaders":{
      "from":[
        "Sender Name <sender@example.com>"
      ],
      "to":[
        "recipient@example.com"
      ],
      "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject":"Message sent from Amazon SES"
    },
    "tags":{
      "ses:configuration-set":[
        "ConfigSet"
      ],
      "ses:source-ip":[
        "192.0.2.0"
      ],
      "ses:from-domain":[
        "example.com"
      ],
      "ses:caller-identity":[
        "ses_user"
      ]
    }
  }
}
```

registre de remise

Voici un exemple d'enregistrement d'`Delivery`événement publié par Amazon SES sur Firehose.

```
{
  "eventType": "Delivery",
  "mail": {
    "timestamp": "2016-10-19T23:20:52.240Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination": [
      "recipient@example.com"
    ],
    "headersTruncated": false,
    "headers": [
```

```
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "text/html; charset=UTF-8"
      },
      {
        "name": "Content-Transfer-Encoding",
        "value": "7bit"
      }
    ],
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "to": [
        "recipient@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES"
    },
    "tags": {
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ],
      "ses:from-domain": [
        "example.com"
```

```
      ],
      "ses:caller-identity": [
        "ses_user"
      ],
      "ses:outgoing-ip": [
        "192.0.2.0"
      ],
      "myCustomTag1": [
        "myCustomTagValue1"
      ],
      "myCustomTag2": [
        "myCustomTagValue2"
      ]
    }
  },
  "delivery": {
    "timestamp": "2016-10-19T23:21:04.133Z",
    "processingTimeMillis": 11893,
    "recipients": [
      "recipient@example.com"
    ],
    "smtpResponse": "250 2.6.0 Message received",
    "reportingMTA": "mta.example.com"
  }
}
```

registre d'envoi

Voici un exemple d'enregistrement d'Sendévénement publié par Amazon SES sur Firehose.

```
{
  "eventType": "Send",
  "mail": {
    "timestamp": "2016-10-14T05:02:16.645Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination": [
      "recipient@example.com"
    ],
    "headersTruncated": false,
    "headers": [
      {
```

```
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "multipart/mixed;  boundary=\"----=_Part_0_716996660.1476421336341\""
      },
      {
        "name": "X-SES-MESSAGE-TAGS",
        "value": "myCustomTag1=myCustomTagValue1, myCustomTag2=myCustomTagValue2"
      }
    ],
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "to": [
        "recipient@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES"
    },
    "tags": {
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ],
      "ses:from-domain": [
        "example.com"
      ],
```

```
      "ses:caller-identity": [
        "ses_user"
      ],
      "myCustomTag1": [
        "myCustomTagValue1"
      ],
      "myCustomTag2": [
        "myCustomTagValue2"
      ]
    }
  },
  "send": {}
}
```

registre de rejet

Voici un exemple d'enregistrement d'`Reject`événement publié par Amazon SES sur Firehose.

```
{
  "eventType": "Reject",
  "mail": {
    "timestamp": "2016-10-14T17:38:15.211Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination": [
      "sender@example.com"
    ],
    "headersTruncated": false,
    "headers": [
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
```

```
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "multipart/mixed; boundary=\"qMm9M+Fa2AknHoGS\""
      },
      {
        "name": "X-SES-MESSAGE-TAGS",
        "value": "myCustomTag1=myCustomTagValue1, myCustomTag2=myCustomTagValue2"
      }
    ],
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "to": [
        "recipient@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES"
    },
    "tags": {
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:caller-identity": [
        "ses_user"
      ],
      "myCustomTag1": [
        "myCustomTagValue1"
      ],
      "myCustomTag2": [
        "myCustomTagValue2"
      ]
    }
  },
  "reject": {
```

```
    "reason": "Bad content"
  }
}
```

registre d'ouverture

Voici un exemple d'enregistrement d'0penévénement publié par Amazon SES sur Firehose.

```
{
  "eventType": "Open",
  "mail": {
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES",
      "to": [
        "recipient@example.com"
      ]
    },
    "destination": [
      "recipient@example.com"
    ],
    "headers": [
      {
        "name": "X-SES-CONFIGURATION-SET",
        "value": "ConfigSet"
      },
      {
        "name":"X-SES-MESSAGE-TAGS",
        "value":"myCustomTag1=myCustomValue1, myCustomTag2=myCustomValue2"
      },
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
```

```
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "multipart/alternative; boundary=\"XBoundary\""
      }
    ],
    "headersTruncated": false,
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "sendingAccountId": "123456789012",
    "source": "sender@example.com",
    "tags": {
      "myCustomTag1":[
        "myCustomValue1"
      ],
      "myCustomTag2":[
        "myCustomValue2"
      ],
      "ses:caller-identity": [
        "IAM_user_or_role_name"
      ],
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ]
    },
    "timestamp": "2017-08-09T21:59:49.927Z"
  },
  "open": {
    "ipAddress": "192.0.2.1",
    "timestamp": "2017-08-09T22:00:19.652Z",
    "userAgent": "Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X)
 AppleWebKit/603.3.8 (KHTML, like Gecko) Mobile/14G60"
  }
}
```

registre de clic

Voici un exemple d'enregistrement d'`Click`événement publié par Amazon SES sur Firehose.


```
{
  "eventType": "Click",
  "click": {
    "ipAddress": "192.0.2.1",
    "link": "http://docs.aws.amazon.com/ses/latest/DeveloperGuide/send-email-
smtp.html",
    "linkTags": {
      "samplekey0": [
        "samplevalue0"
      ],
      "samplekey1": [
        "samplevalue1"
      ]
    },
    "timestamp": "2017-08-09T23:51:25.570Z",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/60.0.3112.90 Safari/537.36"
  },
  "mail": {
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES",
      "to": [
        "recipient@example.com"
      ]
    },
    "destination": [
      "recipient@example.com"
    ],
    "headers": [
      {
        "name": "X-SES-CONFIGURATION-SET",
        "value": "ConfigSet"
      },
      {
        "name":"X-SES-MESSAGE-TAGS",
        "value":"myCustomTag1=myCustomValue1, myCustomTag2=myCustomValue2"
```

```
      },
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "multipart/alternative; boundary=\"XBoundary\""
      },
      {
        "name": "Message-ID",
        "value": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000"
      }
    ],
    "headersTruncated": false,
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "sendingAccountId": "123456789012",
    "source": "sender@example.com",
    "tags": {
      "myCustomTag1":[
        "myCustomValue1"
      ],
      "myCustomTag2":[
        "myCustomValue2"
      ],
      "ses:caller-identity": [
        "ses_user"
      ],
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:from-domain": [
```

```
        "example.com"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ]
    },
    "timestamp": "2017-08-09T23:50:05.795Z"
  }
}
```

registre d'échec de rendu

Voici un exemple d'enregistrement d'`Rendering Failure`événement publié par Amazon SES sur Firehose.

```
{
  "eventType":"Rendering Failure",
  "mail":{
    "timestamp":"2018-01-22T18:43:06.197Z",
    "source":"sender@example.com",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "tags":{
      "ses:configuration-set":[
        "ConfigSet"
      ]
    }
  },
  "failure":{
    "errorMessage":"Attribute 'attributeName' is not present in the rendering data.",
    "templateName":"MyTemplate"
  }
}
```

DeliveryDelay record

Voici un exemple d'enregistrement d'`DeliveryDelay`événement publié par Amazon SES sur Firehose.

```
{
  "eventType": "DeliveryDelay",
  "mail":{
    "timestamp":"2020-06-16T00:15:40.641Z",
    "source":"sender@example.com",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "tags":{
      "ses:configuration-set":[
        "ConfigSet"
      ]
    }
  },
  "deliveryDelay": {
    "timestamp": "2020-06-16T00:25:40.095Z",
    "delayType": "TransientCommunicationFailure",
    "expirationTime": "2020-06-16T00:25:40.914Z",
    "delayedRecipients": [{
      "emailAddress": "recipient@example.com",
      "status": "4.4.1",
      "diagnosticCode": "smtp; 421 4.4.1 Unable to connect to remote host"
    }]
  }
}
```


Abonnement

Voici un exemple d'enregistrement d'`Subscription`événement publié par Amazon SES sur Firehose.


```
{
  "eventType": "Subscription",
  "mail": {
    "timestamp": "2022-01-12T01:00:14.340Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLEe4bccb684-777bc8de-afa7-4970-92b0-f515137b1497-000000",
```

```
    "destination": ["recipient@example.com"],
    "headersTruncated": false,
    "headers": [
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "text/html; charset=UTF-8"
      },
      {
        "name": "Content-Transfer-Encoding",
        "value": "7bit"
      }
    ],
    "commonHeaders": {
      "from": ["sender@example.com"],
      "to": ["recipient@example.com"],
      "messageId": "EXAMPLEe4bccb684-777bc8de-afa7-4970-92b0-f515137b1497-000000",
      "subject": "Message sent from Amazon SES"
    },
    "tags": {
      "ses:operation": ["SendEmail"],
      "ses:configuration-set": ["ConfigSet"],
      "ses:source-ip": ["192.0.2.0"],
      "ses:from-domain": ["example.com"],
      "ses:caller-identity": ["ses_user"],
      "myCustomTag1": ["myCustomValue1"],
      "myCustomTag2": ["myCustomValue2"]
    }
  },
```

```
  "subscription": {
    "contactList": "ContactListName",
    "timestamp": "2022-01-12T01:00:17.910Z",
    "source": "UnsubscribeHeader",
    "newTopicPreferences": {
      "unsubscribeAll": true,
      "topicSubscriptionStatus": [
        {
          "topicName": "ExampleTopicName",
          "subscriptionStatus": "OptOut"
        }
      ]
    },
    "oldTopicPreferences": {
      "unsubscribeAll": false,
      "topicSubscriptionStatus": [
        {
          "topicName": "ExampleTopicName",
          "subscriptionStatus": "OptOut"
        }
      ]
    }
  }
}
```

Interprétation des données d'événement Amazon SES à partir d'Amazon SNS

Amazon SES publie les événements d'envoi d'e-mails dans Amazon Simple Notification Service (Amazon SNS) sous forme de registres JSON. Amazon SNS transmet ensuite les notifications aux points de terminaison abonnés à la rubrique Amazon SNS associée à la destination de l'événement. Pour plus d'informations sur la configuration des rubriques et des abonnements dans Amazon SNS, veuillez consulter Getting Started (Mise en route) dans le Guide du développeur d'Amazon Simple Notification Service.

Pour obtenir une description des contenus de registre et des exemples de registre, consultez les sections suivantes.

- Contenu des registres d'événements
- Exemples de registre d'événement

Contenu des données d'événement publiées par Amazon SES dans Amazon SNS

Amazon SES publie les registres d'événements d'envoi d'e-mails dans Amazon Simple Notification Service au format JSON.

Vous pouvez trouver des exemples de registres pour tous ces types de notifications dans Exemples de données d'événement publiées par Amazon SES sur Amazon SNS.

Rubriques de cette section :

Objet JSON de niveau supérieur

L'objet JSON de niveau supérieur d'un registre d'événement d'envoi d'e-mail contient les champs suivants. Le type d'événement détermine quels autres objets sont présents.

Nom de champ	Description
`eventType`	Chaîne qui décrit le type d'événement. Valeurs possibles : `Bounce`, `Complaint` , `Delivery`, `Send`, `Reject`, `Open`, `Click`, `Rendering Failure`, `DeliveryDelay` ou `Subscription` .

Nom de champ	Description
	Si vous n'avez pas effectué la Configuration de la publication d'événements, ce champ est nommé `notificationType` .
`mail`	Objet JSON qui contient des informations sur l'e-mail qui a généré l'événement.
`bounce`	Ce champ est présent uniquement si `eventType` a la valeur `Bounce`. Il contient des informations sur le retour à l'expéditeur.
`complaint`	Ce champ est présent uniquement si `eventType` a la valeur `Complaint` . Il contient des informations sur la réclamation.
`delivery`	Ce champ est présent uniquement si `eventType` a la valeur `Delivery`. Il contient des informations sur la remise.
`send`	Ce champ est présent uniquement si `eventType` a la valeur `Send`.
`reject`	Ce champ est présent uniquement si `eventType` a la valeur `Reject`. Il contient des informations sur le rejet.
`open`	Ce champ est présent uniquement si `eventType` a la valeur `Open`. Il contient des informations sur l'événement ouvert.
`click`	Ce champ est présent uniquement si `eventType` a la valeur `Click`. Il contient des informations sur l'événement de clic.

Nom de champ	Description
`failure`	Ce champ est présent uniquement si `eventType` a la valeur `Rendering Failure`. Il contient des informations sur l'événement d'échec d'affichage.
`deliveryDelay`	Ce champ est présent uniquement si `eventType` a la valeur `DeliveryDelay`. Il contient des informations sur la livraison différée d'un e-mail.
`subscription`	Ce champ est présent uniquement si `eventType` a la valeur `Subscription`. Il contient des informations sur les préférences d'abonnement.

Objet de l'e-mail

Chaque registre d'événement d'envoi d'e-mail contient des informations sur l'e-mail d'origine dans l'objet `mail`. L'objet JSON qui contient les informations sur un objet `mail` comporte les champs suivants.

Nom de champ	Description
`timestamp`	Date et heure au format ISO8601 (AAAA-MM-JJThh:mm:ss.sZ) auxquelles le message a été envoyé.
`messageId`	ID unique attribué par Amazon SES au message. Amazon SES vous a renvoyé cette valeur lorsque vous avez envoyé le message. **Note** Cet ID de message a été attribué par Amazon SES. Vous trouverez l'ID de message de l'e-mail d'origine dans

Nom de champ	Description
	les champs `headers` et `commonHeaders` de l'objet `mail`.
`source`	Adresse e-mail à partir de laquelle le message a été envoyé (adresse MAIL FROM de l'enveloppe).
`sourceArn`	ARN (Amazon Resource Name) de l'identité qui a été utilisée pour envoyer l'e-mail. Dans le cas d'une autorisation d'envoi, `sourceArn` correspond à l'ARN de l'identité dont le propriétaire a autorisé l'utilisation pour l'envoi de l'e-mail par l'expéditeur délégué. Pour en savoir plus sur l'autorisation d'envoi, consultez Méthodes d'authentification d'e-mail.
`sendingAccountId`	ID de compte AWS du compte utilisé pour envoyer l'e-mail. Dans le cas de l'autorisation d'envoi, `sendingAccountId` correspond à l'ID de compte de l'expéditeur délégué.
`destination`	Liste des adresses e-mail destinataires de l'e-mail original.
`headersTruncated`	Chaîne qui spécifie si les en-têtes ont été tronqués dans la notification, ce qui a lieu s'ils ont une taille supérieure à 10 Ko. Les valeurs possibles sont `true` et `false`.

Nom de champ	Description
`headers`	Liste des en-têtes d'origine de l'e-mail. Chaque en-tête de la liste a un champ `name` et un champ `value`. **Note** Tout ID de message du champ `headers` provient du message d'origine que vous avez transmis à Amazon SES. L'ID de message qu'Amazon SES a ensuite affecté au message se trouve dans le champ `messageId` de l'objet `mail`.
`commonHeaders`	Mappage des en-têtes originaux de l'e-mail communément utilisés. **Note** Tout ID de message contenu dans le champ `commonHeaders` correspond à l'ID de message qu'Amazon SES a par la suite affecté au message dans le champ `messageId` de l'objet `mail`.
`tags`	Une liste des identifications associées à l'e-mail.

Objet bounce

L'objet JSON qui contient les informations sur un événement `Bounce` comporte les champs suivants.

Nom de champ	Description
`bounceType`	Type de retour à l'expéditeur, tel que déterminé par Amazon SES.
`bounceSubType`	Sous-type de retour à l'expéditeur, tel que déterminé par Amazon SES.
`bouncedRecipients`	Liste qui contient les informations sur les destinataires de l'e-mail d'origine ayant fait l'objet d'un retour à l'expéditeur.
`timestamp`	Date et heure au format ISO8601 (AAAA-MM-JJThh:mm:ss.sZ) auxquelles l'ISP a envoyé la notification de retour à l'expéditeur.
`feedbackId`	ID unique du retour à l'expéditeur.
`reportingMTA`	Valeur du champ `Reporting-MTA` du DSN. Il s'agit de la valeur de la MTA qui a tenté d'effectuer l'opération de remise, de relais ou de passerelle décrite dans le DSN. **Note** Ce champ n'apparaît que si une notification de statut de livraison (DSN) a été attachée au retour à l'expéditeur.

Destinataires à l'origine d'un retour à l'expéditeur

Un événement de retour à l'expéditeur peut se rapporter à un seul destinataire ou à plusieurs destinataires. Le champ `bouncedRecipients` contient une liste d'objets (un objet par destinataire dont l'adresse e-mail a généré un retour à l'expéditeur), ainsi que le champ suivant.

Nom de champ	Description
`emailAddress`	Adresse e-mail du destinataire. Si un DSN est disponible, l'adresse correspond à la valeur du champ `Final-Recipient` du DSN.

En outre, si un DSN est attaché au retour à l'expéditeur, les champs suivants peuvent également être présents.

Nom de champ	Description
`action`	Valeur du champ `Action` du DSN. Cette valeur indique l'action effectuée par la MTA de suivi comme résultat de sa tentative de remettre le message à ce destinataire.
`status`	Valeur du champ `Status` du DSN. Il s'agit du code de statut indépendant du transport par destinataire qui indique le statut de remise du message.
`diagnosticCode`	Code de statut émis par la MTA de suivi. Il s'agit de la valeur du champ `Diagnostic-Code` du DSN. Ce champ peut être absent du DSN (et donc également absent du JSON).

Types de retour à l'expéditeur

Chaque évènement de retour à l'expéditeur présente l'un des types affichés dans le tableau suivant.

Le système de publication d'événements ne publie que les retours à l'expéditeur définitifs ou temporaires qui ne sont plus retentés par Amazon SES. Lorsque vous recevez des retours à l'expéditeur marqués `Permanent`, vous devez supprimer les adresses e-mail correspondantes de votre liste de diffusion ; vous ne pourrez plus leur envoyer d'e-mails à l'avenir. Des retours à l'expéditeur `Transient` vous sont envoyés lorsqu'un message a fait plusieurs fois l'objet d'un message d'erreur temporaire, et qu'Amazon SES a arrêté toute tentative de remise. Plus tard, vous

aurez peut-être la possibilité de renvoyer avec succès l'e-mail à une adresse ayant dans un premier temps généré un retour à l'expéditeur `Transient`.

bounceType	bounceSubType	Description
`Undetermined`	`Undetermined`	Amazon SES n'a pas pu déterminer de motif de retour à l'expéditeur.
`Permanent`	`General`	Amazon SES a reçu un message d'erreur définitif général. Si vous recevez ce type de retour à l'expéditeur, vous devez supprimer l'adresse e-mail du destinataire de votre liste de diffusion.
`Permanent`	`NoEmail`	Amazon SES a reçu un message d'erreur définitif, car l'adresse e-mail cible n'existe pas. Si vous recevez ce type de retour à l'expédit eur, vous devez supprimer l'adresse e-mail du destinataire de votre liste de diffusion.
`Permanent`	`Suppressed`	Amazon SES a supprimé l'envoi à cette adresse, car elle a un historique récent de retour à l'expéditeur sous la forme d'adresse non valide. Pour remplacer la liste de suppressi on globale, consultez Utilisation de la liste de suppression au niveau du compte Amazon SES.
`Permanent`	`OnAccountSuppressi onList`	Amazon SES a supprimé l'envoi à cette adresse car celle-ci figure dans la liste de suppression au niveau du compte. Cela n'est pas pris en compte dans votre métrique de taux de retours à l'expéditeur.
`Transient`	`General`	Amazon SES a reçu un retour à l'expéditeur général. Vous pouvez réessayer avec succès l'envoi à ce destinataire à l'avenir.

bounceType	bounceSubType	Description
`Transient`	`MailboxFull`	Amazon SES a reçu un retour à l'expéditeur de boîte aux lettres pleine. Vous pouvez réessayer avec succès l'envoi à ce destinataire à l'avenir.
`Transient`	`MessageTooLarge`	Amazon SES a reçu un message de retour à l'expéditeur trop volumineux. Vous pouvez réessayer avec succès l'envoi à ce destinataire si vous réduisez la taille du message.
`Transient`	`ContentRejected`	Amazon SES a reçu un retour à l'expéditeur de contenu rejeté. Vous pouvez réessayer avec succès l'envoi à ce destinataire si vous modifiez le contenu du message.
`Transient`	`AttachmentRejected`	Amazon SES a reçu un retour à l'expéditeur de pièce jointe rejetée. Vous pouvez réessayer avec succès l'envoi à ce destinataire si vous supprimez ou modifiez la pièce jointe.

Objet de réclamation

L'objet JSON qui contient les informations sur un événement `Complaint` comporte les champs suivants.

Nom de champ	Description
`complainedRecipients`	Liste contenant des informations sur les destinataires qui ont soumis la réclamation.
`timestamp`	Date et heure au format ISO8601 (AAAA-MM-JJThh:mm:ss.sZ) auxquelles l'ISP a envoyé la notification de réclamation.
`feedbackId`	ID unique de la réclamation.

Nom de champ	Description
`complaintSubType`	Sous-type de la réclamation, tel que déterminé par Amazon SES.

De plus, si un rapport de commentaire est attaché à la réclamation, les champs suivants peuvent être présents.

Nom de champ	Description
`userAgent`	Valeur du champ `User-Agent` du rapport de commentaires. Cette valeur indique le nom et la version du système ayant généré le rapport.
`complaintFeedbackType`	Valeur du champ `Feedback-Type` du rapport de commentaires reçu de l'ISP. La valeur contient le type de commentaires.
`arrivalDate`	Valeur du champ `Arrival-Date` ou `Received-Date` du rapport de commentaires au format ISO8601 (YYYY-MM-DDThh:mm:ss.sZ). Le champ peut être absent du rapport (et donc également absent du JSON).

Destinataires à l'origine d'une réclamation

Le champ `complainedRecipients` contient la liste des destinataires susceptibles d'avoir déposé la réclamation.

> **Important**
>
> La plupart des ISP rendent illisibles les adresses e-mail de destinataires qui envoient des réclamations. Pour cette raison, le champ `complainedRecipients` inclut une liste de toutes les personnes auxquelles l'e-mail dont l'adresse est sur le domaine qui a émis la notification de réclamation a été envoyé.

Les objets JSON de cette liste contiennent le champ suivant.

Nom de champ	Description
`emailAddress`	Adresse e-mail du destinataire.

Types de réclamation

Vous pouvez voir les types de réclamation suivants dans le champ `complaintFeedbackType` tels qu'attribués par l'ISP du rapport, selon le site web IANA (Internet Assigned Numbers) :

Nom de champ	Description
`abuse`	Indique un e-mail indésirable ou un autre type d'e-mail malveillant.
`auth-failure`	Rapport d'échec d'authentification d'e-mail.
`fraud`	Indique certains types de fraude ou d'activité d'hameçonnage.
`not-spam`	Indique que l'entité qui fournit le rapport ne considère pas le message en tant que courrier indésirable. Cette option permet de corriger un message qui a été mal balisé ou classé à tort comme courrier indésirable.
`other`	Indique tout autre commentaire ne pouvant être classé dans les autres types enregistrés.
`virus`	Signale qu'un virus a été détecté dans le message d'origine.

Sous-types de réclamation

La valeur du champ `complaintSubType` peut être null ou `OnAccountSuppressionList`. Si la valeur est `OnAccountSuppressionList`, Amazon SES a accepté le message, mais n'a pas essayé de l'envoyer car elle figurait dans la liste de suppression au niveau du compte.

Objet Delivery

L'objet JSON qui contient les informations sur un événement `Delivery` comporte les champs suivants.

Nom de champ	Description
`timestamp`	Date et heure auxquelles Amazon SES a remis l'e-mail au serveur de messagerie du destinataire, au format ISO8601 (AAAA-MM-JJThh:mm:ss.sZ).
`processingTimeMillis`	Délai, en millisecondes, entre le moment où Amazon SES a accepté la demande de l'expéditeur et le moment où Amazon SES a transmis le message au serveur de messagerie du destinataire.
`recipients`	Liste des destinataires auxquels l'événement de remise s'applique.
`smtpResponse`	Message de réponse SMTP du FAI distant ayant accepté l'e-mail depuis Amazon SES. Ce message varie selon l'e-mail, le serveur de messagerie de réception et l'ISP de réception.
`reportingMTA`	Nom d'hôte du serveur de messagerie Amazon SES ayant envoyé l'e-mail.

Objet Send

L'objet JSON qui contient les informations sur un événement `send` est toujours vide.

Objet Reject

L'objet JSON qui contient les informations sur un événement `Reject` comporte les champs suivants.

Nom de champ	Description
`reason`	Raison du rejet de l'e-mail. La seule valeur possible est `Bad content`, ce qui signifie qu'Amazon SES a détecté que l'e-mail contenait un virus. Lorsqu'un message est rejeté, Amazon SES arrête de le traiter et ne tente pas de le remettre au serveur de messagerie du destinataire.

Objet Open

L'objet JSON qui contient les informations sur un événement `Open` comporte les champs suivants.

Nom de champ	Description
`ipAddress`	Adresse IP du destinataire.
`timestamp`	Date et heure auxquelles l'événement open s'est produit, au format ISO8601 (AAAA-MM-JJThh:mm:ss.sZ).
`userAgent`	Agent utilisateur de l'appareil ou client de messagerie que le destinataire a utilisé pour ouvrir l'e-mail.

Objet Click

L'objet JSON qui contient les informations sur un événement `Click` comporte les champs suivants.

Nom de champ	Description
`ipAddress`	Adresse IP du destinataire.
`timestamp`	Date et heure auxquelles l'événement de clic s'est produit, au format ISO8601 (AAAA-MM-JJThh:mm:ss.sZ).

Nom de champ	Description
`userAgent`	Agent utilisateur du client que le destinataire a utilisé pour cliquer sur un lien dans l'e-mail.
`link`	URL du lien sur lequel le destinataire a cliqué.
`linkTags`	Liste des balises ajoutées au lien à l'aide de l'attribut `ses:tags`. Pour en savoir plus sur l'ajout de balises aux liens de vos e-mails, consultez Q5. Puis-je baliser les liens avec des identificateurs uniques ? dans le FAQ sur les métriques Amazon SES d'envoi d'e-mails.

Objet Rendering Failure

L'objet JSON qui contient les informations sur un événement `Rendering Failure` comporte les champs suivants.

Nom de champ	Description
`templateName`	Nom du modèle utilisé pour envoyer l'e-mail.
`errorMessage`	Message qui fournit des informations supplémentaires sur l'échec d'affichage.

Objet DeliveryDelay

L'objet JSON qui contient les informations sur un événement `DeliveryDelay` comporte les champs suivants.

Nom de champ	Description
`delayType`	Type de retard. Les valeurs possibles sont : • InternalFailure – Un problème Amazon SES interne a entraîné le retard du message.

Nom de champ	Description
	• General – Une défaillance générique s'est produite au cours de la conversation SMTP. • MailboxFull – La boîte aux lettres du destinataire est pleine et ne peut pas recevoir de messages supplémentaires. • SpamDetected – Le serveur de messagerie du destinataire a détecté une grande quantité d'e-mails non sollicités provenant de votre compte. • RecipientServerError – Un problème temporaire avec le serveur de messagerie du destinataire empêche la remise du message. • IPFailure – L'adresse IP qui envoie le message est bloquée ou réduite par le fournisseur de messagerie du destinataire. • TransientCommunicationGeneral – Il y a eu un échec de communication temporaire au cours de la conversation SMTP avec le fournisseur de messagerie du destinataire. • BYOIPHostNameLookupUnavailable – Amazon SES n'a pas pu rechercher le nom d'hôte DNS pour vos adresses IP. Ce type de délai ne se produit que lorsque vous utilisez Bring Your Own IP (Fourniture de vos propres adresses IP). • Undetermined – Amazon SES n'a pas été en mesure de déterminer la raison du retard de livraison. • SendingDeferral – Amazon SES a jugé approprié de reporter le message en interne.
`delayedRecipients`	Objet contenant des informations sur le destinataire de l'e-mail.

Nom de champ	Description
`expirationTime`	Date et heure auxquelles Amazon SES cessera d'essayer de remettre le message. Cette valeur est affichée au format ISO 8601.
`reportingMTA`	Adresse IP de l'agent de transfert de messages (MTA) qui a signalé le retard.
`timestamp`	La date et l'heure auxquelles le retard s'est produit, illustrées au format ISO 8601.

Destinataires retardés

L'objet `delayedRecipients` contient les valeurs suivantes.

Nom de champ	Description
`emailAddress`	Adresse électronique ayant entraîné un retard dans la livraison du message.
`status`	Code d'état SMTP associé au délai de livraison.
`diagnosticCode`	Code de diagnostic fourni par l'agent de transfert de message (MTA) récepteur.

Objet Abonnement

L'objet JSON qui contient les informations sur un événement `Subscription` comporte les champs suivants.

Nom de champ	Description
`contactList`	Nom de la liste sur laquelle figure le contact.

Nom de champ	Description
`timestamp`	Date et heure au format ISO8601 (AAAA-MM-JJThh:mm:ss.sZ) auxquelles l'ISP a envoyé la notification de retour à l'expéditeur.
`source`	Adresse e-mail à partir de laquelle le message a été envoyé (adresse MAIL FROM de l'enveloppe).
`newTopicPreferences`	Structure de données JSON (carte) qui spécifie l'état d'abonnement de toutes les rubriques de la liste de contacts en indiquant le statut après une modification (contact abonné ou désabonné).
`oldTopicPreferences`	Structure de données JSON (carte) qui spécifie le statut d'abonnement de toutes les rubriques de la liste de contacts en indiquant l'état avant la modification (contact souscrit ou désabonné).

Préférences de la nouvelle ou de l'ancienne rubrique

Les objets `newTopicPreferences` et `oldTopicPreferences` contiennent les valeurs suivantes.

Nom de champ	Description
`unsubscribeAll`	Indique si le contact s'est désabonné de toutes les rubriques de la liste de contacts.
`topicSubscriptionStatus`	Spécifie le sujet dans le champ `topicName` et mappe le statut de l'abonnement dans le champ .
`topicDefaultSubscriptionStatus`	Spécifie le sujet dans le champ `topicName` et mappe le statut de l'abonnement dans le champ .

Exemples de données d'événement publiées par Amazon SES sur Amazon SNS

Cette section fournit des exemples de chaque type de registre d'événement d'envoi d'e-mails publié par Amazon SES dans Amazon SNS.

Rubriques de cette section :

> **Note**
>
> Dans les exemples suivants, où un champ `tag` est utilisé, il utilise la publication d'événements via un jeu de configuration pour lequel SES prend en charge la publication d'étiquettes pour tous les types d'événements. Si vous utilisez des notifications de commentaires directement sur l'identité, SES ne publie pas d'étiquettes. Découvrez comment ajouter des étiquettes lors de la création d'un jeu de configuration ou de la modification d'un jeu de configuration.

registre de retour à l'expéditeur

L'exemple suivant présente un registre d'événement `Bounce` publié sur Amazon SNS par Amazon SES.

```
{
  "eventType":"Bounce",
  "bounce":{
    "bounceType":"Permanent",
```

```
    "bounceSubType":"General",
    "bouncedRecipients":[
      {
        "emailAddress":"recipient@example.com",
        "action":"failed",
        "status":"5.1.1",
        "diagnosticCode":"smtp; 550 5.1.1 user unknown"
      }
    ],
    "timestamp":"2017-08-05T00:41:02.669Z",
    "feedbackId":"01000157c44f053b-61b59c11-9236-11e6-8f96-7be8aexample-000000",
    "reportingMTA":"dsn; mta.example.com"
  },
  "mail":{
    "timestamp":"2017-08-05T00:40:02.012Z",
    "source":"Sender Name <sender@example.com>",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "headers":[
      {
        "name":"From",
        "value":"Sender Name <sender@example.com>"
      },
      {
        "name":"To",
        "value":"recipient@example.com"
      },
      {
        "name":"Subject",
        "value":"Message sent from Amazon SES"
      },
      {
        "name":"MIME-Version",
        "value":"1.0"
      },
      {
        "name":"Content-Type",
        "value":"multipart/alternative; boundary=\"----
=_Part_7307378_1629847660.1516840721503\""
```

```
      }
    ],
    "commonHeaders":{
      "from":[
        "Sender Name <sender@example.com>"
      ],
      "to":[
        "recipient@example.com"
      ],
      "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject":"Message sent from Amazon SES"
    },
    "tags":{
      "ses:configuration-set":[
        "ConfigSet"
      ],
      "ses:source-ip":[
        "192.0.2.0"
      ],
      "ses:from-domain":[
        "example.com"
      ],
      "ses:caller-identity":[
        "ses_user"
      ]
    }
  }
}
```

registre de réclamation

L'exemple suivant présente un registre d'événement `Complaint` publié sur Amazon SNS par Amazon SES.

```
{
  "eventType":"Complaint",
  "complaint": {
    "complainedRecipients":[
      {
        "emailAddress":"recipient@example.com"
      }
    ],
    "timestamp":"2017-08-05T00:41:02.669Z",
```

```
    "feedbackId":"01000157c44f053b-61b59c11-9236-11e6-8f96-7be8aexample-000000",
    "userAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/60.0.3112.90 Safari/537.36",
    "complaintFeedbackType":"abuse",
    "arrivalDate":"2017-08-05T00:41:02.669Z"
  },
  "mail":{
    "timestamp":"2017-08-05T00:40:01.123Z",
    "source":"Sender Name <sender@example.com>",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "headers":[
      {
        "name":"From",
        "value":"Sender Name <sender@example.com>"
      },
      {
        "name":"To",
        "value":"recipient@example.com"
      },
      {
        "name":"Subject",
        "value":"Message sent from Amazon SES"
      },
      {
        "name":"MIME-Version","value":"1.0"
      },
      {
        "name":"Content-Type",
        "value":"multipart/alternative; boundary=\"----
=_Part_7298998_679725522.1516840859643\""
      }
    ],
    "commonHeaders":{
      "from":[
        "Sender Name <sender@example.com>"
      ],
      "to":[
        "recipient@example.com"
```

```
      ],
      "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject":"Message sent from Amazon SES"
    },
    "tags":{
      "ses:configuration-set":[
        "ConfigSet"
      ],
      "ses:source-ip":[
        "192.0.2.0"
      ],
      "ses:from-domain":[
        "example.com"
      ],
      "ses:caller-identity":[
        "ses_user"
      ]
    }
  }
}
```

registre de remise

L'exemple suivant présente un registre d'événement `Delivery` publié sur Amazon SNS par Amazon SES.

```
{
  "eventType": "Delivery",
  "mail": {
    "timestamp": "2016-10-19T23:20:52.240Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination": [
      "recipient@example.com"
    ],
    "headersTruncated": false,
    "headers": [
      {
        "name": "From",
        "value": "sender@example.com"
      },
```

```
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "text/html; charset=UTF-8"
      },
      {
        "name": "Content-Transfer-Encoding",
        "value": "7bit"
      }
    ],
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "to": [
        "recipient@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES"
    },
    "tags": {
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:caller-identity": [
        "ses_user"
      ],
```

```
      "ses:outgoing-ip": [
        "192.0.2.0"
      ],
      "myCustomTag1": [
        "myCustomTagValue1"
      ],
      "myCustomTag2": [
        "myCustomTagValue2"
      ]
    }
  },
  "delivery": {
    "timestamp": "2016-10-19T23:21:04.133Z",
    "processingTimeMillis": 11893,
    "recipients": [
      "recipient@example.com"
    ],
    "smtpResponse": "250 2.6.0 Message received",
    "reportingMTA": "mta.example.com"
  }
}
```

registre d'envoi

L'exemple suivant présente un registre d'événement Send publié sur Amazon SNS par Amazon SES. Certains champs ne sont pas toujours présents. Par exemple, avec un e-mail modèle, l'objet est rendu ultérieurement et inclus dans les événements suivants.

```
{
  "eventType": "Send",
  "mail": {
    "timestamp": "2016-10-14T05:02:16.645Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination": [
      "recipient@example.com"
    ],
    "headersTruncated": false,
    "headers": [
      {
        "name": "From",
```

```
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "multipart/mixed;  boundary=\"----=_Part_0_716996660.1476421336341\""
      },
      {
        "name": "X-SES-MESSAGE-TAGS",
        "value": "myCustomTag1=myCustomTagValue1, myCustomTag2=myCustomTagValue2"
      }
    ],
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "to": [
        "recipient@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES"
    },
    "tags": {
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:caller-identity": [
```

```
        "ses_user"
      ],
      "myCustomTag1": [
        "myCustomTagValue1"
      ],
      "myCustomTag2": [
        "myCustomTagValue2"
      ]
    }
  },
  "send": {}
}
```

registre de rejet

L'exemple suivant présente un registre d'événement `Reject` publié sur Amazon SNS par Amazon SES.

```
{
  "eventType": "Reject",
  "mail": {
    "timestamp": "2016-10-14T17:38:15.211Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination": [
      "sender@example.com"
    ],
    "headersTruncated": false,
    "headers": [
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
```

```
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "multipart/mixed; boundary=\"qMm9M+Fa2AknHoGS\""
      },
      {
        "name": "X-SES-MESSAGE-TAGS",
        "value": "myCustomTag1=myCustomTagValue1, myCustomTag2=myCustomTagValue2"
      }
    ],
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "to": [
        "recipient@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES"
    },
    "tags": {
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:caller-identity": [
        "ses_user"
      ],
      "myCustomTag1": [
        "myCustomTagValue1"
      ],
      "myCustomTag2": [
        "myCustomTagValue2"
      ]
    }
  },
```

```
  "reject": {
    "reason": "Bad content"
  }
}
```

registre d'ouverture

L'exemple suivant présente un registre d'événement 0pen publié sur Amazon SNS par Amazon SES.

```
{
  "eventType": "Open",
  "mail": {
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES",
      "to": [
        "recipient@example.com"
      ]
    },
    "destination": [
      "recipient@example.com"
    ],
    "headers": [
      {
        "name": "X-SES-CONFIGURATION-SET",
        "value": "ConfigSet"
      },
      {
        "name":"X-SES-MESSAGE-TAGS",
        "value":"myCustomTag1=myCustomValue1, myCustomTag2=myCustomValue2"
      },
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
```

```
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "multipart/alternative; boundary=\"XBoundary\""
      }
    ],
    "headersTruncated": false,
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "sendingAccountId": "123456789012",
    "source": "sender@example.com",
    "tags": {
      "myCustomTag1":[
        "myCustomValue1"
      ],
      "myCustomTag2":[
        "myCustomValue2"
      ],
      "ses:caller-identity": [
        "IAM_user_or_role_name"
      ],
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ]
    },
    "timestamp": "2017-08-09T21:59:49.927Z"
  },
  "open": {
    "ipAddress": "192.0.2.1",
    "timestamp": "2017-08-09T22:00:19.652Z",
    "userAgent": "Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X)
AppleWebKit/603.3.8 (KHTML, like Gecko) Mobile/14G60"
  }
```

```
}
```

registre de clic

L'exemple suivant présente un registre d'événement `Click` publié sur Amazon SNS par Amazon SES.

```
{
  "eventType": "Click",
  "click": {
    "ipAddress": "192.0.2.1",
    "link": "http://docs.aws.amazon.com/ses/latest/DeveloperGuide/send-email-
smtp.html",
    "linkTags": {
      "samplekey0": [
        "samplevalue0"
      ],
      "samplekey1": [
        "samplevalue1"
      ]
    },
    "timestamp": "2017-08-09T23:51:25.570Z",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/60.0.3112.90 Safari/537.36"
  },
  "mail": {
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES",
      "to": [
        "recipient@example.com"
      ]
    },
    "destination": [
      "recipient@example.com"
    ],
    "headers": [
      {
        "name": "X-SES-CONFIGURATION-SET",
        "value": "ConfigSet"
```

```
      },
      {
        "name":"X-SES-MESSAGE-TAGS",
        "value":"myCustomTag1=myCustomValue1, myCustomTag2=myCustomValue2"
      },
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "multipart/alternative; boundary=\"XBoundary\""
      },
      {
        "name": "Message-ID",
        "value": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000"
      }
    ],
    "headersTruncated": false,
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "sendingAccountId": "123456789012",
    "source": "sender@example.com",
    "tags": {
      "myCustomTag1":[
        "myCustomValue1"
      ],
      "myCustomTag2":[
        "myCustomValue2"
      ],
      "ses:caller-identity": [
        "ses_user"
      ],
```

```
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ]
    },
    "timestamp": "2017-08-09T23:50:05.795Z"
  }
}
```

registre d'échec de rendu

L'exemple suivant présente un registre d'événement `Rendering Failure` publié sur Amazon SNS par Amazon SES.

```
{
  "eventType":"Rendering Failure",
  "mail":{
    "timestamp":"2018-01-22T18:43:06.197Z",
    "source":"sender@example.com",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "tags":{
      "ses:configuration-set":[
        "ConfigSet"
      ]
    }
  },
  "failure":{
    "errorMessage":"Attribute 'attributeName' is not present in the rendering data.",
    "templateName":"MyTemplate"
  }
}
```

DeliveryDelayrecord

L'exemple suivant présente un registre d'événement `DeliveryDelay` publié sur Amazon SNS par Amazon SES.


```
{
  "eventType": "DeliveryDelay",
  "mail":{
    "timestamp":"2020-06-16T00:15:40.641Z",
    "source":"sender@example.com",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "tags":{
      "ses:configuration-set":[
        "ConfigSet"
      ]
    }
  },
  "deliveryDelay": {
    "timestamp": "2020-06-16T00:25:40.095Z",
    "delayType": "TransientCommunicationFailure",
    "expirationTime": "2020-06-16T00:25:40.914Z",
    "delayedRecipients": [{
      "emailAddress": "recipient@example.com",
      "status": "4.4.1",
      "diagnosticCode": "smtp; 421 4.4.1 Unable to connect to remote host"
    }]
  }
}
```


Enregistrement d'abonnement

Voici un exemple d'enregistrement d'`Subscription`événement publié par Amazon SES sur Firehose.


```
{
  "eventType": "Subscription",
  "mail": {
```

```
    "timestamp": "2022-01-12T01:00:14.340Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLEe4bccb684-777bc8de-afa7-4970-92b0-f515137b1497-000000",
    "destination": ["recipient@example.com"],
    "headersTruncated": false,
    "headers": [
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "text/html; charset=UTF-8"
      },
      {
        "name": "Content-Transfer-Encoding",
        "value": "7bit"
      }
    ],
    "commonHeaders": {
      "from": ["sender@example.com"],
      "to": ["recipient@example.com"],
      "messageId": "EXAMPLEe4bccb684-777bc8de-afa7-4970-92b0-f515137b1497-000000",
      "subject": "Message sent from Amazon SES"
    },
    "tags": {
      "ses:operation": ["SendEmail"],
      "ses:configuration-set": ["ConfigSet"],
      "ses:source-ip": ["192.0.2.0"],
      "ses:from-domain": ["example.com"],
```

```
      "ses:caller-identity": ["ses_user"],
      "myCustomTag1": ["myCustomValue1"],
      "myCustomTag2": ["myCustomValue2"]
    }
  },
  "subscription": {
    "contactList": "ContactListName",
    "timestamp": "2022-01-12T01:00:17.910Z",
    "source": "UnsubscribeHeader",
    "newTopicPreferences": {
      "unsubscribeAll": true,
      "topicSubscriptionStatus": [
        {
          "topicName": "ExampleTopicName",
          "subscriptionStatus": "OptOut"
        }
      ]
    },
    "oldTopicPreferences": {
      "unsubscribeAll": false,
      "topicSubscriptionStatus": [
        {
          "topicName": "ExampleTopicName",
          "subscriptionStatus": "OptOut"
        }
      ]
    }
  }
}
```

Surveillance de votre réputation d'expéditeur Amazon SES

Amazon SES suit activement plusieurs métriques qui peuvent nuire à votre réputation d'expéditeur ou provoquer une baisse de vos taux de remise d'e-mails. Dans ce processus, le taux de retours à l'expéditeur et le taux de réclamations constituent deux métriques importantes de votre compte. Si le taux de retours à l'expéditeur ou de réclamations pour votre compte est trop élevé, nous pouvons placer votre compte sous vérification ou suspendre sa capacité à envoyer des e-mails.

Comme les taux de retours à l'expéditeur et de réclamations sont essentiels à l'état de votre compte, Amazon SES comprend une page de métriques de réputation dans la console Amazon SES que vous pouvez utiliser pour suivre ces métriques. Les métriques de réputation peuvent également afficher des informations sur les facteurs non liés aux retours à l'expéditeur ou aux réclamations qui pourraient nuire à votre réputation d'expéditeur. Par exemple, si vous envoyez un e-mail à un piège pour le courrier indésirable connu, un message s'affiche sur le tableau de bord.

Cette section contient des informations sur l'accès aux métriques de réputation, sur l'interprétation des informations qu'il contient et sur la configuration des systèmes afin de vous informer activement des facteurs qui pourraient avoir un impact sur votre réputation d'expéditeur.

Dans cette section, vous allez retrouver les rubriques suivantes :

- Utilisation de métriques de réputation pour suivre les taux de retours à l'expéditeur et de réclamations.
- Messages des métriques de réputation
- Création d'alarmes de surveillance de réputation avec CloudWatch
- Métriques SNDS pour les adresses IP dédiées
- Interruption automatique d'envoi d'e-mails

Utilisation de métriques de réputation pour suivre les taux de retours à l'expéditeur et de réclamations.

La page de la console des métriques de réputation contient les mêmes informations que celles vues par l'équipe Amazon SES pour déterminer l'état des comptes individuels.

Pour afficher les métriques de réputation

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation sur le côté gauche de l'écran, choisissez Reputation Dashboard (Métriques de réputation).

   Le tableau de bord affiche les informations suivantes :

   - Statut du compte (État du compte) — Un résumé de la performance de vos taux de retours à l'expéditeur et de réclamations. Les valeurs possibles incluent :
     - Healthy (Sain) – Aucun problème n'a actuellement un impact sur votre compte.
     - Under review (Vérification en cours) – Votre compte est en cours de vérification. Si les problèmes qui nous ont amenés à placer votre compte en vérification ne sont pas résolus avant la fin de la période de vérification, la capacité de votre compte à envoyer des e-mails peut être suspendue.
     - Pending end of review decision (En attente d'une décision de fin de vérification) – Votre compte est en cours de vérification. En raison de la nature des problèmes qui nous ont amenés à placer votre compte en vérification, nous avons besoin d'effectuer une vérification manuelle de votre compte avant d'exécuter toute autre action.
     - Sending paused (Envoi suspendu) – Nous avons suspendu la capacité de votre compte à envoyer des e-mails. Tant que la capacité de votre compte à envoyer des e-mails est suspendue, vous ne pouvez pas envoyer d'e-mails avec Amazon SES. Vous pouvez nous demander de réviser cette décision. Pour en savoir plus sur la demande d'une révision, veuillez consulter FAQ sur le processus de vérification des envois Amazon SES.
     - Pending sending pause (En attente - Suspension d'envoi) – Votre compte est en cours de vérification. Les problèmes qui nous ont amenés à placer votre compte en vérification n'ont pas été résolus. Dans ce cas, nous suspendons généralement la capacité de votre compte à envoyer des e-mails. Toutefois, en raison de la nature de votre compte, nous devons le vérifier avant que toute autre action ne soit effectuée.
   - Bounce Rate (Taux de retours à l'expéditeur) – Pourcentage d'e-mails envoyés depuis votre compte ayant entraîné un message d'erreur définitif. Consultez comment votre taux de retours est calculé.
   - Complaint Rate (Taux de réclamations) – Pourcentage d'e-mails envoyés depuis votre compte et signalés en tant que courrier indésirable par les destinataires. Consultez comment votre taux de réclamations est calculé.

> **Note**
>
> Les sections Bounce Rate (Taux de retours à l'expéditeur) et Complaint Rate (Taux de réclamations) incluent également des messages d'état pour leurs métriques respectives. La liste suivante contient les messages d'état pouvant s'afficher pour ces métriques :
>
> - Healthy (Sain) – La métrique se trouve au sein des niveaux normaux.
> - Almost healed (Presque réparé) – La métrique a entraîné la vérification de votre compte. Depuis que la période de vérification a commencé, la métrique est restée sous le taux maximal. Si elle reste sous le taux maximal, son statut peut se changer en Healthy (Sain) avant la fin de la période de vérification.
> - Under review (En vérification) – La métrique a entraîné la vérification de votre compte, et se trouve toujours au-dessus du taux maximum. Si le problème à l'origine du fait que la métrique dépasse le taux maximal n'est pas résolu avant la fin de la période de vérification, la capacité de votre compte à envoyer des e-mails peut être suspendue.
> - Sending pause (Suspension d'envoi) – La métrique a entraîné la suspension de la capacité de votre compte à envoyer des e-mails. Lorsque la capacité de votre compte à envoyer des e-mails est suspendue, vous ne pouvez pas envoyer d'e-mails avec Amazon SES. Vous pouvez nous demander de réviser cette décision. Pour de plus amples informations sur l'envoi d'une demande de réexamen, veuillez consulter FAQ sur le processus de vérification des envois Amazon SES.
> - Pending sending pause (En attente - Suspension d'envoi) La métrique a entraîné la vérification de votre compte. Les problèmes à l'origine de cette période de vérification n'ont pas été résolus. Ces problèmes peuvent entraîner la suspension de la capacité de votre compte à envoyer des e-mails. Un membre de l'équipe Amazon SES examinera votre compte avant que toute autre action ne soit prise.

- Other Notifications (Autres notifications) – Si votre compte rencontre des problèmes relatifs à la réputation sans lien avec des retours à l'expéditeur ou des réclamations, un bref message s'affiche ici. Pour en savoir plus sur les notifications qui peuvent s'afficher dans cette zone, consultez Messages des métriques de réputation.

Messages des métriques de réputation

La page de la console de métrique de réputation Amazon SES fournit des métriques importantes liées à votre compte. Les sections suivantes décrivent les messages qui peuvent s'afficher dans ce tableau de bord, et fournissent des conseils et des informations que vous pouvez utiliser pour résoudre les problèmes liés à votre réputation d'expéditeur.

Cette section contient des informations sur les types de notification suivants :

- Messages de statut
- Notification de taux de retours à l'expéditeur
- Notification de taux de réclamations
- Notification d'organisation de lutte anti-spam
- Notification de bombardement de liste
- Notification de commentaire direct
- Notification de liste de blocage de domaines
- Notification de révision en interne
- Notification de fournisseur de boîte aux lettres
- Notification de commentaire de destinataires
- Notification de compte lié
- Notification de piège pour le courrier indésirable
- Notification de site vulnérable
- Notification d'informations d'identification compromises
- Autre notification

Messages de statut

Lorsque vous utilisez la page de la console de métrique de réputation, un message décrivant le statut de votre compte Amazon SES s'affiche. Les informations suivantes répertorient les valeurs de statut de compte possibles :

- Healthy (Sains) – Aucun problème n'a actuellement un impact sur votre compte.

- Under review (Vérification en cours) – Votre compte est en cours de vérification. Si les problèmes qui nous ont amenés à placer votre compte en vérification ne sont pas résolus avant la fin de la période de vérification, la capacité de votre compte à envoyer des e-mails peut être suspendue.
- Pending end of review decision (En attente d'une décision de fin de vérification) – Votre compte est en cours de vérification. En raison de la nature des problèmes qui nous ont amenés à placer votre compte en vérification, nous avons besoin d'effectuer une vérification manuelle de votre compte avant d'exécuter toute autre action.
- Sending paused (Envoi suspendu) – Nous avons suspendu la capacité de votre compte à envoyer des e-mails. Tant que la capacité de votre compte à envoyer des e-mails est suspendue, vous ne pouvez pas envoyer d'e-mails avec Amazon SES. Vous pouvez nous demander de réviser cette décision. Pour en savoir plus sur la demande d'une révision, veuillez consulter FAQ sur le processus de vérification des envois Amazon SES.
- Pending sending pause (En attente - Suspension d'envoi) – Votre compte est en cours de vérification. Les problèmes qui nous ont amenés à placer votre compte en vérification n'ont pas été résolus. Dans ce cas, nous suspendons généralement la capacité de votre compte à envoyer des e-mails. Toutefois, en raison de la nature de votre compte, nous devons le vérifier avant que toute autre action ne soit effectuée.

De plus, les sections Bounce Rate (Taux de retour à l'expéditeur) et Complaint Rate (Taux de réclamation) de la page des métriques de réputation affichent des récapitulatifs de statut pour leurs métriques respectives. Les informations suivantes répertorient les valeurs de statut de métrique possibles :

- Healthy (Sain) – La métrique se trouve au sein des niveaux normaux.
- Almost healed (Presque réparé) – La métrique a entraîné la vérification de votre compte. Depuis que la période de vérification a commencé, la métrique est restée sous le taux maximal. Si elle reste sous le taux maximal, son statut peut se changer en Healthy (Sain) avant la fin de la période de vérification.
- Under review (En vérification) – La métrique a entraîné la vérification de votre compte, et se trouve toujours au-dessus du taux maximum. Si le problème à l'origine du fait que la métrique dépasse le taux maximal n'est pas résolu avant la fin de la période de vérification, la capacité de votre compte à envoyer des e-mails peut être suspendue.
- Sending pause (Suspension d'envoi) – La métrique a entraîné la suspension de la capacité de votre compte à envoyer des e-mails. Lorsque la capacité de votre compte à envoyer des e-mails est suspendue, vous ne pouvez pas envoyer d'e-mails avec Amazon SES. Vous pouvez nous

demander de réviser cette décision. Pour de plus amples informations sur l'envoi d'une demande de réexamen, veuillez consulter FAQ sur le processus de vérification des envois Amazon SES.

- Pending sending pause (En attente - Suspension d'envoi) La métrique a entraîné la vérification de votre compte. Les problèmes à l'origine de cette période de vérification n'ont pas été résolus. Ces problèmes peuvent entraîner la suspension de la capacité de votre compte à envoyer des e-mails. Un membre de l'équipe Amazon SES examinera votre compte avant que toute autre action ne soit prise.

Notification de taux de retours à l'expéditeur

Cette section contient des informations supplémentaires sur les notifications de taux de retours à l'expéditeur présentées dans la page des métriques de la réputation Amazon SES.

Pourquoi avez-vous reçu cette notification ?

Vous avez reçu cette notification car le taux de retours à l'expéditeur de votre compte était trop élevé. Le taux de retours à l'expéditeur est basé sur le nombre de messages d'erreur définitifs générés par votre compte Amazon SES. Les fournisseurs de messagerie interprètent un taux élevé de retours à l'expéditeur comme le signe que ce dernier ne gère pas correctement sa liste de destinataires et qu'il est susceptible d'envoyer des e-mails indésirables.

Un message d'erreur définitif se produit lorsqu'un e-mail est envoyé à une adresse qui n'existe pas. Amazon SES ne prend pas en compte dans ce calcul les messages d'erreur temporaire, qui se produisent lorsque l'adresse d'un destinataire est temporairement dans l'impossibilité de recevoir vos messages. Les e-mails non remis que vous envoyez à des adresses et domaines vérifiés, ainsi que ceux que vous envoyez au simulateur de boîte aux lettres (mailbox) Amazon SES, ne sont pas non plus pris en compte dans ce calcul.

Nous calculons votre taux de retours à l'expéditeur en fonction d'un volume représentatif d'e-mails. Un volume représentatif est une quantité d'e-mails qui représentent vos pratiques d'envoi habituelles. Afin d'être équitable à la fois pour les expéditeurs de volumes élevés et faibles, le volume représentatif est différent pour chaque compte et évolue avec les tendances d'envoi de ce dernier.

Pour obtenir de meilleurs résultats, maintenez un taux de retours à l'expéditeur inférieur à 5 %. Les taux de retour à l'expéditeur supérieurs peuvent avoir un impact sur la remise de vos e-mails. Si votre taux de retour est de 5 % ou plus, nous placerons automatiquement votre compte sous vérification. Si votre taux de retour à l'expéditeur est de 10 % ou plus, nous pouvons suspendre la capacité de votre

compte à envoyer d'autres e-mails tant que vous n'avez pas résolu le problème à l'origine de ce taux élevé.

Ce que vous pouvez faire pour résoudre ce problème

Si ce n'est pas déjà fait, mettez en place un processus pour capturer et gérer les retours à l'expéditeur et les réclamations. Tous les comptes Amazon SES doivent bénéficier de ces processus. Pour de plus amples informations, veuillez consulter Métriques de la réussite pour les programmes de messagerie.

Ensuite, déterminez les adresses e-mail à l'origine des retours à l'expéditeur, puis créez et mettez en place un plan pour réduire ou éliminer ces retours. Si la capacité de votre compte à envoyer des e-mails est déjà suspendue, connectez-vous à AWS Management Console Console et accédez au AWS Support. Répondez au cas que nous avons ouvert en votre nom.

Si votre compte est en cours d'examen

A la fin de la période de vérification, si le taux de retours à l'expéditeur reste supérieur à 10 % pour votre compte, nous pouvons suspendre la capacité de votre compte à envoyer des e-mails jusqu'à ce que vous ayez résolu le problème.

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Dans votre réponse au cas, décrivez les modifications que vous avez mises en œuvre. Si nous pensons que les modifications réduiront votre taux de retours à l'expéditeur, nous ajusterons nos calculs afin de prendre en compte uniquement les retours à l'expéditeur reçus après la mise en œuvre de ces modifications.

Si la capacité de votre compte à envoyer des e-mails est suspendue

Vous pouvez demander que nous reconsidérions cette décision. Pour de plus amples informations, veuillez consulter FAQ sur le processus de vérification des envois Amazon SES.

Lorsque vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Spécifiez en détail les actions entreprises pour résoudre ce problème, ainsi que les plans détaillés vous assurant que ce problème ne se reproduira pas. Après avoir reçu votre demande, nous examinons les informations que vous avez fournies et modifions le statut de votre compte, le cas échéant.

Notification de taux de réclamations

Cette section contient des informations supplémentaires sur les notifications de taux de réclamations présentées dans la page des métriques de la réputation Amazon SES.

Pourquoi avez-vous reçu cette notification ?

Vous avez reçu cette notification parce que le taux de réclamations concernant votre compte était trop élevé. Le taux de réclamations est basé sur le nombre de réclamations générées par votre compte Amazon SES. La plupart des fournisseurs de messagerie interprètent un taux élevé de réclamations comme le signe que ce dernier ne gère pas correctement sa liste de destinataires et qu'il est susceptible d'envoyer des e-mails indésirables.

Une réclamation se produit lorsqu'un destinataire identifie comme spam un e-mail que vous avez envoyé. Cela se produit généralement lorsque le destinataire utilise le bouton « Signaler le spam » dans son client de messagerie. Les réclamations générées par les e-mails que vous envoyez au simulateur de boîte au lettres (mailbox) Amazon SES ne sont pas prises en compte dans ce calcul.

Nous calculons votre taux de réclamations en fonction d'un volume représentatif d'e-mails. Un volume représentatif est une quantité d'e-mails qui représentent vos pratiques d'envoi habituelles. Afin d'être équitable à la fois pour les expéditeurs de volumes élevés et faibles, le volume représentatif est différent pour chaque compte et évolue avec les tendances d'envoi de ce dernier.

Pour obtenir de meilleurs résultats, maintenez un taux de réclamations inférieur à 0,1 %. Des taux de réclamation supérieurs peuvent avoir un impact sur la remise de vos e-mails. Si votre taux de réclamations est de 0,1 % ou plus, nous placerons automatiquement votre compte sous vérification. Si votre taux de réclamations est de 0,5 % ou plus, nous pouvons suspendre la capacité de votre compte à envoyer d'autres e-mails tant que vous n'avez pas résolu le problème à l'origine de ce taux élevé.

Ce que vous pouvez faire pour résoudre ce problème

Si ce n'est pas déjà fait, mettez en place un processus pour capturer et gérer les retours à l'expéditeur et les réclamations. Tous les comptes Amazon SES doivent bénéficier de ces processus. Pour de plus amples informations, veuillez consulter Métriques de la réussite pour les programmes de messagerie.

Ensuite, déterminez quels sont les messages envoyés qui entraînent des réclamations, et mettez en œuvre un plan afin de réduire ces réclamations. Si la capacité de votre compte à envoyer des e-mails

est déjà suspendue, connectez-vous à la Console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom.

Bien que vous deviez immédiatement arrêter d'envoyer des e-mails aux adresses à l'origine des réclamations, il est important d'identifier les facteurs qui ont amené les destinataires à formuler les réclamations. Une fois que vous avez identifié ces facteurs, ajustez votre comportement d'envoi d'e-mails en conséquence.

Si votre compte est en cours d'examen

À la fin de la période de vérification, si le taux de réclamations reste supérieur à 0,5 % pour votre compte, nous pouvons suspendre la capacité de votre compte à envoyer des e-mails jusqu'à ce que vous ayez résolu le problème.

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Dans votre réponse au cas, décrivez les modifications que vous avez mises en œuvre. Si nous pensons que les modifications réduiront votre taux de réclamations, nous ajusterons nos calculs afin de prendre en compte uniquement les réclamations reçues après la mise en œuvre de ces modifications.

Si la capacité de votre compte à envoyer des e-mails est suspendue

Vous pouvez demander que nous reconsidérions cette décision. Pour de plus amples informations, veuillez consulter FAQ sur le processus de vérification des envois Amazon SES.

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Spécifiez en détail les actions entreprises pour résoudre ce problème, ainsi que les plans détaillés vous assurant que ce problème ne se reproduira pas. Après avoir reçu votre demande, nous examinons les informations que vous avez fournies et modifions le statut de votre compte, le cas échéant.

Notification d'organisation de lutte anti-spam

Cette section contient des informations supplémentaires sur les notifications d'organisation de lutte anti-spam présentées dans la page des métriques de réputation Amazon SES.

Pourquoi avez-vous reçu cette notification ?

Une organisation de lutte anti-spam reconnue a rapporté que certains contenus envoyés depuis votre compte Amazon SES ont été signalés comme indésirables ou problématiques par leurs systèmes.

Nous ne sommes pas en mesure de fournir des informations sur les messages spécifiques qui ont amené l'organisation de lutte anti-spam à signaler votre contenu comme étant problématique. Nous ne pouvons pas fournir le nom de l'organisation qui a émis le rapport. En général, les organisations de lutte anti-spam prennent en compte une combinaison des facteurs suivants : commentaires du destinataire, métriques d'intérêt des messages, tentatives de livraison de message à des adresses non valides, contenu signalé par leurs filtres anti-spam et accès aux pièges pour courrier indésirable. Cette liste n'est pas exhaustive ; ces organisations peuvent signaler votre contenu pour d'autres raisons.

Ce que vous pouvez faire pour résoudre ce problème

Pour résoudre ce problème, vous devez déterminer les aspects de votre programme d'envoi d'e-mails qui peuvent amener les organisations de lutte anti-spam à signaler vos e-mails comme problématiques. Vous devez ensuite modifier votre programme d'envoi pour répondre à ces problèmes.

Si votre compte est en cours d'examen

À la fin de la période de vérification, si l'organisation de lutte anti-spam continue d'identifier les e-mails envoyés à partir de votre compte comme problématiques, nous pouvons suspendre la capacité de votre compte à envoyer des e-mails jusqu'à ce que vous ayez résolu le problème.

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Dans votre message, fournissez le détail des changements apportés. Lorsque nous recevons ces informations, nous prolongeons la période de vérification afin de nous assurer que nous analysons uniquement les notifications de l'organisation de lutte anti-spam reçues après la mise en œuvre de vos modifications. À la fin de la prolongation de la période de vérification, si votre compte n'est plus répertorié par l'organisation de lutte anti-spam, nous supprimons la vérification de votre compte.

Si la capacité de votre compte à envoyer des e-mails est suspendue

Vous pouvez demander que nous reconsidérions cette décision. Pour de plus amples informations, veuillez consulter FAQ sur le processus de vérification des envois Amazon SES.

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Spécifiez en détail les actions entreprises pour résoudre ce problème, ainsi que les plans détaillés vous assurant que ce problème ne se reproduira pas. Après avoir reçu votre demande, nous examinons les informations que vous avez fournies et modifions le statut de votre compte, le cas échéant.

Notification de bombardement de liste

Cette section contient des informations supplémentaires sur les notifications de bombardement de liste présentées dans la page des métriques de réputation Amazon SES.

Pourquoi avez-vous reçu cette notification ?

Une organisation antispam a identifié que vos processus d'envoi d'e-mails sont vulnérables au « bombardement de liste ». Le bombardement de liste est une forme d'attaque au cours de laquelle un hacker enregistre un très grand nombre d'adresses e-mail sur un formulaire web. Le bombardement de liste peut entraîner des perturbations de service pour les utilisateurs des services de messagerie concernés. Cela peut également entraîner le blocage de votre e-mail par les fournisseurs de messagerie.

Les organisations antispam utilisent des méthodes propriétaires pour identifier les sites vulnérables au bombardement de liste. C'est la raison pour laquelle nous ne pouvons pas fournir de détails supplémentaires sur le problème qui a conduit l'organisation antispam à identifier votre processus d'envoi d'e-mails comme problématique. Nous ne pouvons pas partager le nom de l'organisation qui a identifié le problème.

Ce que vous pouvez faire pour résoudre ce problème

Vous devez examiner tous vos formulaires d'inscription web pour vous assurer qu'ils ne sont pas vulnérables à ce type d'attaque. Chaque formulaire doit inclure un CAPTCHA pour empêcher les scripts automatisés de soumettre des demandes d'abonnement. De plus, lorsque de nouveaux utilisateurs s'inscrivent à votre produit ou service, envoyez-leur un e-mail pour confirmer qu'ils ont effectivement l'intention de s'inscrire. N'envoyez aucun e-mail supplémentaire aux clients à moins qu'ils n'acceptent explicitement vos communications.

Enfin, vous devez effectuer un « laissez-passer d'autorisation » sur votre liste de diffusion. Dans un laissez-passer d'autorisation, vous envoyez un e-mail à tous vos clients pour leur demander s'ils souhaitent toujours recevoir des e-mails de votre part. Envoyez les e-mails uniquement aux clients qui confirment qu'ils souhaitent continuer à en recevoir de votre part.

Si votre compte est en cours d'examen

À la fin de la période de vérification, si l'organisation de lutte anti-spam continue d'identifier les e-mails envoyés à partir de votre compte comme problématiques, nous pouvons suspendre la capacité de votre compte à envoyer des e-mails jusqu'à ce que vous ayez résolu le problème.

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Dans votre message, fournissez le détail des changements apportés. Lorsque nous recevons ces informations, nous prolongeons la période de vérification afin de nous assurer que nous analysons uniquement les notifications de l'organisation de lutte anti-spam reçues après la mise en œuvre de vos modifications. À la fin de la prolongation de la période de vérification, si votre compte n'est plus répertorié par l'organisation de lutte anti-spam, nous supprimons la vérification de votre compte.

Si la capacité de votre compte à envoyer des e-mails est suspendue

Vous pouvez demander que nous reconsidérions cette décision. Pour de plus amples informations, veuillez consulter FAQ sur le processus de vérification des envois Amazon SES.

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Spécifiez en détail les actions entreprises pour résoudre ce problème, ainsi que les plans détaillés vous assurant que ce problème ne se reproduira pas. Après avoir reçu votre demande, nous examinons les informations que vous avez fournies et modifions le statut de votre compte, le cas échéant.

Notification de commentaire direct

Cette section contient des informations supplémentaires sur les notifications de commentaire direct présentées dans la page des métriques de réputation Amazon SES.

Pourquoi avez-vous reçu cette notification ?

Un nombre important d'utilisateurs ont contacté directement Amazon SES pour signaler la réception de messages en provenance d'une adresse ou d'un domaine associé à votre compte Amazon SES. Ce type de commentaire n'est pas visible dans les réclamations signalées directement par les fournisseurs de boîte aux lettres ; de même, il n'est pas inclus dans les métriques de retour à l'expéditeur et de réclamation affichées sur la page des métriques de réputation.

Pour protéger la confidentialité des utilisateurs ayant signalé ces problèmes, nous ne pouvons pas fournir leurs adresses e-mail.

Les destinataires peuvent se plaindre auprès d'Amazon SES lorsqu'ils reçoivent des messages pour lesquels ils ne se sont pas inscrits, lorsqu'ils ne reçoivent pas le type d'e-mail qu'ils s'attendent à recevoir, lorsqu'ils trouvent que les e-mails qu'ils reçoivent ne sont pas utiles ou intéressants, lorsqu'ils ne reconnaissent pas que les messages qu'ils reçoivent font suite à leur inscription, ou lorsqu'ils reçoivent un trop grand nombre de messages. Cette liste n'est pas exhaustive ; les facteurs pertinents dans votre cas dépendent de votre programme d'envoi d'e-mails spécifique.

Ce que vous pouvez faire pour résoudre ce problème

Nous vous recommandons de mettre en place une stratégie de confirmation de l'acceptation, comme décrit dans Création et gestion de vos listes, pour l'acquisition de nouvelles adresses, et d'envoyer des e-mails uniquement aux adresses ayant validé le processus de confirmation de l'acceptation.

De plus, vous devez purger vos listes d'adresses qui n'ont pas interagi récemment avec vos e-mails. Vous pouvez utiliser le suivi d'ouverture et de clic, comme décrit dans Surveillance de votre activité d'envoi Amazon SES, pour déterminer quels sont les utilisateurs qui affichent et interagissent avec le contenu que vous envoyez.

Si votre compte est en cours d'examen

À la fin de la période de vérification, si Amazon SES continue de recevoir un nombre élevé de réclamations directes sur les messages envoyés à partir de votre compte, nous pouvons suspendre la capacité de votre compte à envoyer des e-mails jusqu'à ce que vous ayez résolu le problème.

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Fournissez des informations détaillées sur les étapes que vous avez effectuées pour résoudre le problème et décrivez la manière dont ces étapes empêchent que le problème ne se reproduise. Si nous jugeons que les modifications que vous avez effectuées traitent correctement le problème, nous annulons la période de vérification de votre compte.

Si la capacité de votre compte à envoyer des e-mails est suspendue

Vous pouvez demander que nous reconsidérions cette décision. Pour de plus amples informations, veuillez consulter FAQ sur le processus de vérification des envois Amazon SES.

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous

avons ouvert en votre nom. Spécifiez en détail les actions entreprises pour résoudre ce problème, ainsi que les plans détaillés vous assurant que ce problème ne se reproduira pas. Après avoir reçu votre demande, nous examinons les informations que vous avez fournies et modifions le statut de votre compte, le cas échéant.

Notification de liste de blocage de domaines

Cette section contient des informations supplémentaires sur les notifications de liste de blocage de domaines présentées dans la page des métriques de réputation Amazon SES.

Pourquoi avez-vous reçu cette notification ?

Les e-mails envoyés depuis votre compte Amazon SES contiennent des références à des domaines qui ont été répertoriés sur une liste de blocage de domaines reconnue. Les domaines figurant sur ces listes sont généralement associés à des comportements abusifs ou malveillants. Les domaines en question peuvent être ou ne pas être les domaines à partir desquels vous envoyez des e-mails. Les messages qui incluent des références ou des liens vers un domaine figurant sur une liste de blocage, ou qui incluent des images hébergées sur un domaine de ce type, peuvent également être signalés.

Nous ne sommes pas en mesure de fournir les noms des domaines à l'origine du signalement de votre message ou d'identifier les e-mails ayant été signalés de cette manière.

Ce que vous pouvez faire pour résoudre ce problème

Tout d'abord, créez une liste de tous les domaines référencés dans les e-mails que vous envoyez via Amazon SES. Ensuite, utilisez l'outil de recherche de domaines Spamhaus pour déterminer quels domaines de votre messagerie figurent sur la liste de blocage de domaines. Plusieurs domaines référencés dans les e-mails que vous envoyez peuvent figurer sur cette liste de blocage.

La liste de blocage de domaines Spamhaus n'est pas affiliée à Amazon SES ou AWS. Nous ne pouvons donner aucune garantie quant à l'exactitude des domaines de cette liste. La propriété, l'utilisation et la maintenance des outils de recherche de domaines et de liste de blocage de domaines Spamhaus sont détenues par le projet Spamhaus.

Si votre compte est en cours d'examen

Nous recherchons des références à des domaines qui ont été utilisés à des fins malveillantes dans les e-mails que vous envoyez pendant la période de révision. Si vos e-mails contiennent toujours un nombre important de références à ces domaines, nous pouvons suspendre la capacité de votre compte à envoyer des e-mails jusqu'à ce que vous ayez résolu le problème.

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Dans votre message, fournissez le détail des changements apportés. Lorsque nous recevons ces informations, nous prolongeons la période de vérification afin de nous assurer que nous analysons uniquement le nombre de domaines figurant sur la liste de blocage et référencés dans vos e-mails après la mise en œuvre de vos modifications. À la fin de la prolongation de cette période de vérification, si le nombre de notifications de liste de blocage de domaines a été réduite ou éliminée, et que nous pensons que vous avez pris des mesures pour éviter que ce problème ne se reproduise, nous annulons la période de vérification pour votre compte.

Si la capacité de votre compte à envoyer des e-mails est suspendue

Vous pouvez demander que nous reconsidérions cette décision. Pour de plus amples informations, veuillez consulter FAQ sur le processus de vérification des envois Amazon SES.

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Spécifiez en détail les actions entreprises pour résoudre ce problème, ainsi que les plans détaillés vous assurant que ce problème ne se reproduira pas. Après avoir reçu votre demande, nous examinons les informations que vous avez fournies et modifions le statut de votre compte, le cas échéant.

Notification de révision en interne

Cette section contient des informations supplémentaires sur les notifications de révision en interne présentées dans la page des métriques de réputation Amazon SES.

Pourquoi avez-vous reçu cette notification ?

Une révision complète de votre compte a identifié plusieurs caractéristiques qui peuvent amener les fournisseurs de boîte aux lettres ou les destinataires à identifier vos messages en tant que courrier indésirable.

Afin de protéger nos processus de détection d'actes abusifs, nous ne pouvons pas révéler les facteurs spécifiques ayant conduit votre compte à être signalé de cette manière.

Parmi les facteurs communs pouvant conduire à cette détermination, on peut citer :

- Les messages signalés par des systèmes anti-spam commerciaux.

- Le contenu des messages impliquant que le destinataire n'a pas explicitement demandé à recevoir l'e-mail.
- Les incompatibilités entre l'expéditeur du message et les personnalisations dans le corps de l'e-mail.
- Le contenu qui empêche l'expéditeur d'être identifié de manière évidente.
- L'envoi de messages dont le contenu est associé aux e-mails indésirables.
- Le formatage de schémas associés aux e-mails indésirables.
- L'envoi à partir de domaines de mauvaise réputation, ou la référence à ces domaines dans les e-mails.

Cette liste n'est pas exhaustive. La raison spécifique de cette notification peut être une combinaison de plusieurs de ces facteurs, mais également un motif non répertorié.

Ce que vous pouvez faire pour résoudre ce problème

Les suggestions suivantes peuvent vous aider à réduire la gravité du problème :

- Assurez-vous que les seuls destinataires que vous contactez sont ceux qui ont explicitement demandé à recevoir des e-mails de votre part.
- N'achetez pas, ne louez pas, n'empruntez pas de listes de destinataires.
- Ne tentez pas de masquer votre identité ou le sujet de votre communication dans les messages que vous envoyez.
- Créez une liste de tous les domaines référencés dans les e-mails que vous envoyez via Amazon SES, puis utilisez l'outil de recherche de domaine Spamhaus, disponible à l'adresse https://www.spamhaus.org/lookup/ pour déterminer si l'un des domaines se trouve sur la liste de blocage des domaines.
- Veillez à suivre les bonnes pratiques du secteur lors de la conception de vos e-mails.

Cette liste n'est pas exhaustive, mais elle devrait vous aider à identifier certains facteurs parmi les plus courants pouvant conduire au signalement de vos e-mails.

La liste de blocage de domaines Spamhaus n'est pas affiliée à Amazon SES ou AWS. Nous ne pouvons donner aucune garantie quant à l'exactitude des domaines de cette liste. La propriété, l'utilisation et la maintenance des outils de recherche de domaines et de liste de blocage de domaines Spamhaus sont détenues par le projet Spamhaus.

Si votre compte est en cours de révision ou si la capacité de votre compte à envoyer des e-mails est suspendue

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Fournissez des informations détaillées sur les étapes que vous avez effectuées pour résoudre le problème et décrivez la manière dont ces étapes empêchent que le problème ne se reproduise. Si nous jugeons que les modifications que vous avez effectuées traitent correctement le problème, nous annulons la période de vérification ou nous mettons fin à la suspension d'envoi à partir de votre compte.

Si nous supprimons une période de vérification ou une interruption d'envoi depuis votre compte, et que nous observons le même problème ultérieurement, nous pouvons placer à nouveau votre compte sous révision ou suspendre votre capacité à envoyer des e-mails à nouveau. Dans des cas extrêmes, ou si nous observons des exemples répétés du même problème, nous pouvons suspendre de façon définitive la capacité de votre compte à envoyer des e-mails.

Veuillez consulter FAQ sur le processus de vérification des envois Amazon SES pour de plus amples informations sur les actions à mettre en œuvre si votre compte est en cours de révision ou que la capacité de votre compte à envoyer des e-mails est suspendue.

Notification de fournisseur de boîte aux lettres

Cette section contient des informations supplémentaires sur les notifications de fournisseur de boîte aux lettres présentées dans la page des métriques de réputation Amazon SES.

Pourquoi avez-vous reçu cette notification ?

Un important fournisseur de boîte aux lettres nous a signalé que des e-mails indésirables ou malveillants sont envoyés à partir d'une adresse ou d'un domaine associé à votre compte Amazon SES.

Nous ne pouvons pas partager l'identité de l'organisation à l'origine de ce rapport. De plus, nous ne disposons d'aucune information relative aux facteurs spécifiques qui ont amené le fournisseur de boîte aux lettres à émettre le rapport. En général, les fournisseurs de boîte aux lettres procèdent à ce type de détermination en fonction des commentaires des clients, des métriques d'engagement des clients, des tentatives de livraison de message à des adresses non valides, et du contenu signalé par des filtres anti-spam. Cette liste n'est pas exhaustive ; d'autres facteurs peuvent entraîner le signalement de votre contenu par le fournisseur de boîte aux lettres.

Ce que vous pouvez faire pour résoudre ce problème

Pour résoudre ce problème, vous devez déterminer les aspects de votre programme d'envoi d'e-mails qui peuvent amener les fournisseurs de boîte aux lettres à signaler vos e-mails comme problématiques. Vous devez ensuite modifier votre programme d'envoi pour répondre à ces problèmes.

Si votre compte est en cours d'examen

À la fin de la période de vérification, si le fournisseur de boîte aux lettes continue d'identifier les e-mails envoyés à partir de votre compte comme problématiques, nous pouvons suspendre la capacité de votre compte à envoyer des e-mails jusqu'à ce que vous ayez résolu le problème.

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Dans votre message, fournissez le détail des changements apportés. Lorsque nous recevons ces informations, nous prolongeons la période de vérification afin de nous assurer que nous analysons uniquement le nombre de notifications de fournisseur de boîte aux lettres reçues après la mise en œuvre de vos modifications. Si, à la fin de la prolongation de la période de vérification, votre compte n'est plus signalé comme problématique par le fournisseur de boîte aux lettres, il est possible que nous supprimions la vérification de votre compte.

Si la capacité de votre compte à envoyer des e-mails est suspendue

Vous pouvez demander que nous reconsidérions cette décision. Pour de plus amples informations, veuillez consulter FAQ sur le processus de vérification des envois Amazon SES.

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Spécifiez en détail les actions entreprises pour résoudre ce problème, ainsi que les plans détaillés vous assurant que ce problème ne se reproduira pas. Après avoir reçu votre demande, nous examinons les informations que vous avez fournies et modifions le statut de votre compte, le cas échéant.

Notification de commentaire de destinataires

Cette section contient des informations supplémentaires sur les notifications de commentaire du destinataire présentées dans la page des métriques de réputation Amazon SES.

Pourquoi avez-vous reçu cette notification ?

Un important fournisseur de boîte aux lettres nous a signalé qu'un grand nombre de ses utilisateurs a identifié des e-mails envoyés depuis votre compte Amazon SES comme indésirables. Ce type de commentaire n'est pas visible dans les réclamations signalées directement par les fournisseurs de boîte aux lettres ; de même, il n'est pas inclus dans les notifications de retour à l'expéditeur et de réclamation Amazon SES.

Un grand nombre de réclamations peut avoir un impact négatif sur tous les utilisateurs Amazon SES. Pour protéger votre réputation et celle des autres clients Amazon SES, nous prenons des mesures immédiates lorsqu'un compte reçoit un certain nombre de réclamations.

Nous ne sommes pas en mesure de fournir la liste des adresses e-mail spécifiques qui signalent vos e-mails comme indésirables. De plus, nous ne sommes pas en mesure de partager le nom du fournisseur de boîte aux lettres qui nous a signalé ce problème.

Ce que vous pouvez faire pour résoudre ce problème

Pour résoudre ce problème, vous devez déterminer les aspects de votre programme d'envoi d'e-mails qui peuvent amener vos destinataires à formuler des réclamations contre les messages qu'ils reçoivent de votre part. Une fois que vous avez identifié ces facteurs, ajustez vos pratiques d'envoi d'e-mails en conséquence.

Pour acquérir de nouvelles adresses, nous vous recommandons de mettre en place une stratégie de confirmation de l'acceptation, comme décrit dans Création et gestion de vos listes. Nous vous recommandons d'envoyer des e-mails uniquement aux adresses ayant validé le processus de confirmation de l'acceptation.

De plus, vous devez purger vos listes d'adresses qui n'ont pas interagi récemment avec vos e-mails. Vous pouvez utiliser le suivi d'ouverture et de clic, comme décrit dans Surveillance de votre activité d'envoi Amazon SES, pour déterminer quels sont les utilisateurs qui affichent et interagissent avec le contenu que vous envoyez.

Si votre compte est en cours d'examen

À la fin de la période de vérification, si le fournisseur de boîte aux lettres continue de signaler un nombre élevé de réclamations, nous pouvons suspendre la capacité de votre compte à envoyer des e-mails jusqu'à ce que vous ayez résolu le problème.

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous

avons ouvert en votre nom. Dans votre message, fournissez le détail des changements apportés. Lorsque nous recevons ces informations, nous prolongeons la période de vérification afin de nous assurer que nous analysons uniquement le nombre de réclamations de fournisseur de boîte aux lettres reçues après la mise en œuvre de vos modifications. À la fin de la prolongation de cette période de vérification, si le nombre de réclamations de fournisseur de boîte aux lettres a été réduit ou éliminé, il est possible que nous mettions fin à la vérification de votre compte.

Si la capacité de votre compte à envoyer des e-mails est suspendue

Vous pouvez demander que nous reconsidérions cette décision. Pour de plus amples informations, veuillez consulter FAQ sur le processus de vérification des envois Amazon SES.

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Spécifiez en détail les actions entreprises pour résoudre ce problème, ainsi que les plans détaillés vous assurant que ce problème ne se reproduira pas. Après avoir reçu votre demande, nous examinons les informations que vous avez fournies et modifions le statut de votre compte, le cas échéant.

Notification de compte lié

Cette section contient des informations supplémentaires sur les notifications de compte lié présentées dans la page des métriques de réputation Amazon SES.

Pourquoi avez-vous reçu cette notification ?

Nous avons détecté de graves problèmes en relation avec les e-mails envoyés depuis un autre compte Amazon SES. Nous pensons que le compte problématique est lié à votre Compte AWS ; nous avons donc pris des mesures afin d'éviter les problèmes similaires.

Ce que vous pouvez faire pour résoudre ce problème

Lorsque nous suspendons la capacité d'un compte à envoyer des e-mails, nous envoyons toujours des informations sur les raisons de la pause au propriétaire du compte. Reportez-vous à l'e-mail que nous avons envoyé au propriétaire du compte lié Pour en savoir plus.

Traitez en premier les problèmes relatifs au compte lié. Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Fournissez des

informations détaillées sur les étapes que vous avez effectuées pour résoudre le problème et décrivez la manière dont ces étapes empêchent que le problème ne se reproduise. Si nous jugeons que les modifications que vous avez effectuées traitent correctement le problème, nous annulons la période de vérification ou nous mettons fin à la suspension d'envoi à partir de votre compte.

Notification de piège pour le courrier indésirable

Cette section contient des informations supplémentaires sur les notifications de piège pour le courrier indésirable présentées dans la page de métriques de réputation Amazon SES.

Pourquoi avez-vous reçu cette notification ?

Une organisation de lutte anti-spam tiers nous a signalé que leurs adresses de piège pour le courrier indésirable ont récemment reçu un e-mail en provenance d'une adresse ou d'un domaine vérifié associé à votre compte Amazon SES.

Un piège pour le courrier indésirable est une adresse e-mail dormante utilisée exclusivement pour attirer les e-mails indésirables. Un grand nombre de rapports de piège pour le courrier indésirable peut avoir un impact négatif sur tous les utilisateurs Amazon SES. Pour protéger votre réputation et celle des autres clients Amazon SES, nous prenons des mesures immédiates lorsqu'un compte envoie un volume particulier d'e-mails à des adresses de piège pour le courrier indésirable.

Ce que vous pouvez faire pour résoudre ce problème

Nous ne pouvons pas divulguer les adresses e-mail associées au piège pour le courrier indésirable que vous avez rencontré. Ces adresses sont étroitement surveillés par les organisations qui en sont propriétaires ; une fois qu'elles sont connues, elles deviennent inutiles.

L'envoi d'e-mails à des adresses de piège pour le courrier indésirable indiquent généralement un problème lié à la manière dont vous obtenez les adresses e-mail de vos clients. Par exemple, des listes d'adresses e-mail achetées peuvent contenir des adresses de piège pour le courrier indésirable ; c'est la raison pour laquelle l'envoi d'e-mails à des listes achetées ou louées est interdit par les conditions d'utilisation Amazon SES. Pour acquérir de nouvelles adresses, nous vous recommandons de mettre en place une stratégie de confirmation de l'acceptation, comme décrit dans Création et gestion de vos listes. Nous vous recommandons d'envoyer des e-mails uniquement aux adresses ayant validé le processus de confirmation de l'acceptation.

De plus, vous devez purger vos listes d'adresses qui n'ont pas interagi récemment avec vos e-mails. Vous pouvez utiliser le suivi d'ouverture et de clic, comme décrit dans Surveillance de votre activité

d'envoi Amazon SES, pour déterminer quels sont les utilisateurs qui affichent et interagissent avec le contenu que vous envoyez.

Si votre compte est en cours d'examen

À la fin de la période de vérification, si des messages continuent à être envoyés depuis votre compte aux adresses des pièges pour le courrier indésirable, nous pouvons suspendre la capacité de votre compte à envoyer des e-mails jusqu'à ce que vous ayez résolu le problème.

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Dans votre message, fournissez le détail des changements apportés. Lorsque nous recevons ces informations, nous prolongeons la période de vérification afin de nous assurer que nous analysons uniquement le nombre de rapports de piège pour le courrier indésirable reçus après la mise en œuvre de vos modifications. À la fin de la prolongation de cette période de vérification, si le nombre de rapports de piège pour le courrier indésirable a été réduit ou éliminé, il est possible que nous mettions fin à la vérification de votre compte.

Si la capacité de votre compte à envoyer des e-mails est suspendue

Vous pouvez demander que nous reconsidérions cette décision. Pour de plus amples informations, veuillez consulter FAQ sur le processus de vérification des envois Amazon SES.

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Spécifiez en détail les actions entreprises pour résoudre ce problème, ainsi que les plans détaillés vous assurant que ce problème ne se reproduira pas. Après avoir reçu votre demande, nous examinons les informations que vous avez fournies et modifions le statut de votre compte, le cas échéant.

Notification de site vulnérable

Cette section contient des informations supplémentaires sur les notifications de site vulnérable présentées dans la page de métriques de réputation Amazon SES.

Pourquoi avez-vous reçu cette notification ?

Un examen complet a déterminé que des messages ont été envoyés depuis votre compte, mais nous pensons que vous n'avez pas eu l'intention de les envoyer. Ces messages sont fortement

susceptibles d'être signalés comme du courrier indésirable par les fournisseurs de boîte aux lettres et les destinataires.

Dans la plupart des cas, un tiers abuse d'une fonction de votre site Web pour envoyer des e-mails indésirables. Par exemple, si votre site Web contient une fonction « envoyer à un ami », « contactez-nous », « inviter un ami » ou une fonction similaire, un tiers peut l'utiliser pour envoyer des e-mails indésirables.

Ce que vous pouvez faire pour résoudre ce problème

Tout d'abord, identifiez les fonctions de votre site web ou de vos applications qui peuvent permettre à un tiers d'envoyer des e-mails à l'aide d'Amazon SES à votre insu. Dans le cas de votre Centre de support, vous pouvez demander un échantillon des messages que nous pensons avoir envoyés de cette manière.

Ensuite, modifiez votre application ou votre site Web pour empêcher les envois indésirables. Par exemple, ajoutez une image CAPTCHA, limitez la vitesse à laquelle les e-mails peuvent être envoyés, supprimez la possibilité pour les utilisateurs de soumettre du contenu personnalisé, exigez que les utilisateurs se connectent pour envoyer des e-mails et supprimez la possibilité pour l'application de générer plusieurs notifications simultanées.

Si votre compte est en cours de révision ou si la capacité de votre compte à envoyer des e-mails est suspendue

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Spécifiez en détail les actions entreprises pour résoudre ce problème, ainsi que les plans détaillés vous assurant que ce problème ne se reproduira pas. Après avoir reçu votre demande, nous examinons les informations que vous avez fournies et modifions le statut de votre compte, le cas échéant.

Si nous supprimons une période de vérification ou une interruption d'envoi depuis votre compte, et que nous observons le même problème ultérieurement, nous pouvons placer à nouveau votre compte sous révision ou suspendre votre capacité à envoyer des e-mails à nouveau. Si nous constatons des problèmes très graves ou des exemples répétés du même problème, nous pouvons suspendre de façon définitive la capacité de votre compte à envoyer des e-mails.

Veuillez consulter FAQ sur le processus de vérification des envois Amazon SES pour de plus amples informations sur les actions à mettre en œuvre si votre compte est en cours de révision ou que la capacité de votre compte à envoyer des e-mails est suspendue.

Notification d'informations d'identification compromises

Cette section contient des informations supplémentaires sur les notifications d'informations d'identification compromises présentées dans la page des métriques de la réputation Amazon SES.

Pourquoi avez-vous reçu cette notification ?

Un examen complet a déterminé que des messages ont été envoyés depuis votre compte, mais nous pensons que vous n'avez pas eu l'intention de les envoyer. Ces messages sont fortement susceptibles d'être signalés comme du courrier indésirable par les fournisseurs de boîte aux lettres et les destinataires.

Certaines causes courantes sont des clés d'accès IAM compromises, des mots de passe SMTP compromis ou d'autres vulnérabilités de sécurité.

Ce que vous pouvez faire pour résoudre ce problème

Vous devez procéder à un examen complet de la sécurité de vos mécanismes d'utilisation de SES. Vérifiez que vous avez procédé à la rotation de tous les mots de passe applicables ou SMTP et que vous avez supprimé tout utilisateur ou ressource non autorisé de votre compte. Assurez-vous que vous ne stockez pas d'informations sensibles telles que des mots de passe ou des clés d'accès sur des sites web ou des référentiels tiers. Il est désormais recommandé de ne pas utiliser de clés d'accès IAM pour les utilisateurs, et jamais pour l'utilisateur root. Si vous les utilisez encore, vous devez les migrer vers des mécanismes qui fournissent des informations d'identification temporaires, comme la création d'un utilisateur dans AWS IAM Identity Center.

Si votre compte est en cours de révision ou si la capacité de votre compte à envoyer des e-mails est suspendue

Si vous avez mis en œuvre des changements qui permettront, selon vous, de résoudre le problème, connectez-vous à la console AWS et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Spécifiez en détail les actions entreprises pour résoudre ce problème, ainsi que les plans détaillés vous assurant que ce problème ne se reproduira pas. Après avoir reçu votre demande, nous examinons les informations que vous avez fournies et modifions le statut de votre compte, le cas échéant.

Si nous supprimons une période de vérification ou une interruption d'envoi depuis votre compte, et que nous observons le même problème ultérieurement, nous pouvons placer à nouveau votre

compte sous révision ou suspendre votre capacité à envoyer des e-mails à nouveau. Si nous constatons des problèmes très graves ou des exemples répétés du même problème, nous pouvons suspendre de façon définitive la capacité de votre compte à envoyer des e-mails.

Veuillez consulter FAQ sur le processus de vérification des envois Amazon SES pour de plus amples informations sur les actions à mettre en œuvre si votre compte est en cours de révision ou que la capacité de votre compte à envoyer des e-mails est suspendue.

Autre notification

Cette section contient des informations supplémentaires sur d'autres notifications présentées dans la page de métriques de réputation Amazon SES.

Pourquoi avez-vous reçu cette notification ?

Un examen humain ou automatique a identifié des problèmes qui ne sont pas répertoriés dans les sections précédentes de ce document.

Ce que vous pouvez faire pour résoudre ce problème

Reportez-vous au cas du Centre de support que nous avons ouvert en votre nom Pour en savoir plus sur le problème spécifique. Pour accéder au Centre de support, connectez-vous à AWS Management Console, puis choisissez Centre de support. Dans votre réponse au cas, décrivez les modifications que vous avez mises en œuvre. En fonction de votre situation spécifique et de la nature des problèmes identifiés, nous pouvons mettre fin à la période de révision ou restaurer la capacité de votre compte à envoyer des e-mails.

Création d'alarmes de surveillance de réputation avec CloudWatch

Amazon SES publie automatiquement une série de métriques relatives à la réputation sur Amazon CloudWatch. Vous pouvez utiliser ces métriques pour créer des alarmes qui vous informent lorsque votre taux de retours à l'expéditeur ou de réclamations atteint des niveaux susceptibles d'avoir un impact sur votre capacité à envoyer des e-mails.

> **Note**
>
> La partie CloudWatch des procédures de cette section n'est destinée qu'à présenter les principales étapes de la configuration d'une alarme CloudWatch pour surveiller votre

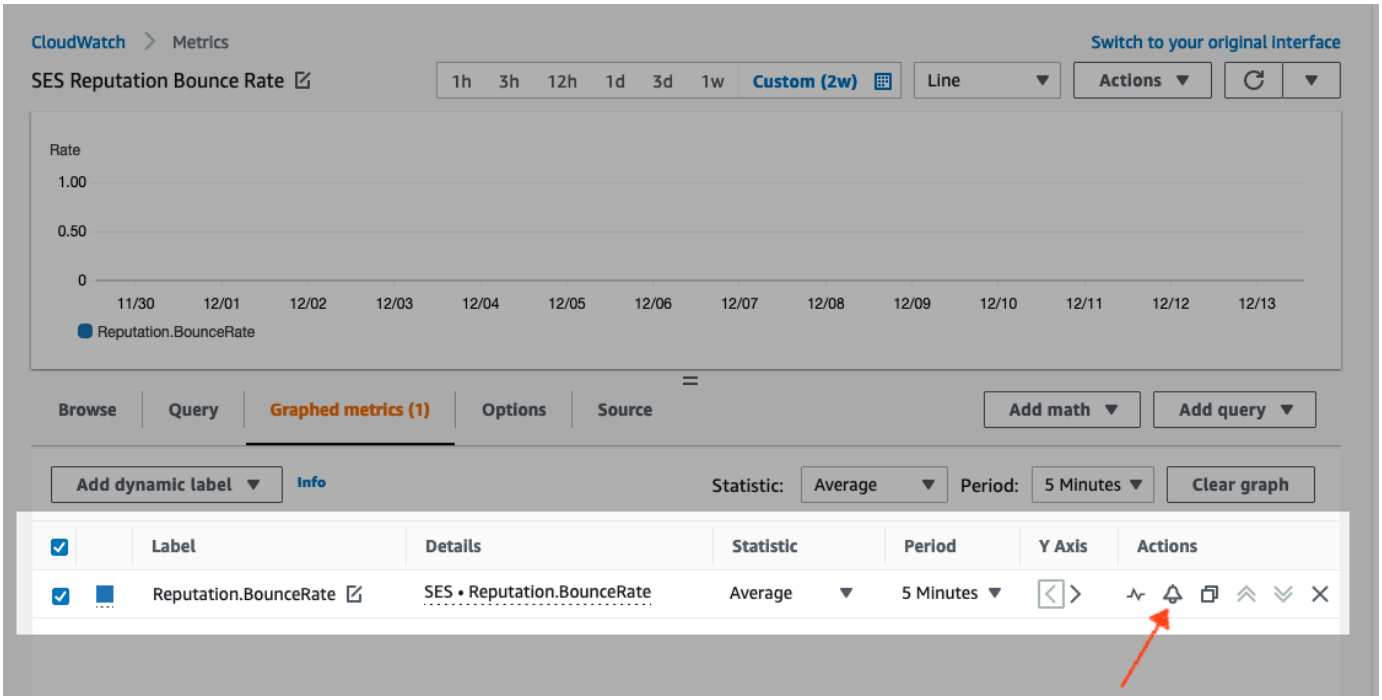
réputation d'expéditeur SES. Elles n'abordent pas les configurations avancées relatives aux paramètres facultatifs des alarmes CloudWatch. Pour des informations complètes sur l'utilisation des alarmes CloudWatch, consultez Utilisation des alarmes Amazon CloudWatch dans le Guide de l'utilisateur Amazon CloudWatch.

Prérequis

- Créez une rubrique Amazon SNS, puis abonnez-vous à celle-ci par l'intermédiaire du point de terminaison de votre choix (e-mail ou SMS). Pour plus d'informations, veuillez consulter les sections Créer une rubrique et Abonnement d'un point de terminaison à une rubrique Amazon SNS, dans le Guide du développeur d'Amazon Simple Notification Service.
- Si vous n'avez jamais envoyé de courrier électronique dans la région actuelle, vous ne consulterez peut-être pas l'espace de noms SES. Pour vous assurer que vous disposez des métriques, envoyez un e-mail de test au simulateur de boîte aux lettres.

Pour créer une alarme CloudWatch pour surveiller la réputation d'envoi

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Dans le panneau de navigation sur le côté gauche de l'écran, choisissez Reputation Dashboard (Métriques de réputation).
3. Sur la page Métriques de réputation, dans l'onglet Niveau du compte, dans le panneau Taux de retours à l'expéditeur ou Taux de réclamations, choisissez Afficher dans CloudWatch. La console CloudWatch s'ouvre avec la métrique choisie.
4. Dans l'onglet Graphed metrics (Graphique des métriques), sur la ligne de la métrique choisie, en l'occurrence ici,Reputation.BounceRate, choisissez l'icône de cloche dans la colonne Actions (voir l'image ci-dessous). Cela ouvrira la page Specify metric and conditions (Spécification des métriques et conditions.



5. Faites défiler jusqu'au panneau Conditions et choisissez Static (Statique) dans le champ Threshold type (Type de seuil).

   a. Dans le champ Whenever ***metric*** is... (Chaque fois que la métrique est…), choisissez Greater/Equal (Plus grand/Égal).

   b. Dans le champ than (que), spécifiez la valeur qui doit amener CloudWatch à déclencher une alarme.

      - Si vous créez une alarme pour surveiller votre taux de retours à l'expéditeur, notez qu'Amazon SES recommande un taux de retours à l'expéditeur de moins de 5 %. Si le taux de retours à l'expéditeur pour votre compte est supérieur à 10 %, nous pouvons suspendre temporairement la capacité de votre compte à envoyer des e-mails. Pour cette raison, vous devez configurer CloudWatch de sorte qu'il vous envoie une notification lorsque le taux de retours à l'expéditeur pour votre compte est supérieur ou égal à 0,05 (5 %).
      - Si vous créez une alarme pour surveiller votre taux de réclamations, notez qu'Amazon SES recommande un taux de réclamations de moins de 0,1 %. Si le taux de réclamations pour votre compte est supérieur à 0,5 %, nous pouvons suspendre temporairement la capacité de votre compte à envoyer des e-mails. Pour cette raison, vous devez configurer CloudWatch de sorte qu'il vous envoie une notification lorsque le taux de réclamations pour votre compte est supérieur ou égal à 0,001 (0,1 %).

c. Développez Additional configuration (Configuration supplémentaire) et choisissez Treat missing data as ignore (maintain the alarm state) [Traiter les données manquantes en les ignorant (conserver l'état de l'alarme) dans le champ Missing data treatment (Traitement des données manquantes).

d. Choisissez Next (Suivant).

6. Dans le panneau Configure actions (Configuration d'actions), choisissez In alarm (avec alarme), dans le champ Alarm state trigger (déclencheur d'état d'alarme).

   a. Choisissez Select an existing SNS topic (Sélectionner une rubrique SNS existante), dans le champ Select an SNS topic (Sélectionner une rubrique SNS).

   b. Choisissez la rubrique que vous avez créée et à laquelle vous vous êtes abonné lors de la phase préalable dans la zone de recherche Send notification to (Envoyer une notification à).

   c. Choisissez Next (Suivant).

7. Dans le panneau Add a name and description (Ajouter un nom et une description), entrez un nom et une description pour l'alarme, puis choisissez Next (Suivant).

8. Dans le panneau Preview and create (Afficher un aperçu et créer), vérifiez vos paramètres et, si vous êtes satisfait, choisissez Create alarm (Créer une alarme). Si vous vous souhaitez modifier quelque chose, sélectionnez le bouton Previous (Précédent) pour chaque section à laquelle vous souhaitez retourner pour effectuer des modifications.

Métriques SNDS pour les adresses IP dédiées

Vous pouvez afficher les données SNDS (Smart Network Data Services) pour les adresses IP dédiées louées dans chaque Région AWS où vous utilisez Amazon SES. Ces données SNDS sont disponibles via la console Amazon CloudWatch.

SNDS est un programme Outlook qui aide les propriétaires d'adresses IP à prévenir le courrier indésirable dans leur espace d'adresses IP. Amazon SES fournit ces données importantes aux personnes qui louent des adresses IP dédiées. Les données SNDS fournissent des informations sur le comportement d'envoi d'e-mails d'une adresse IP et signalent les sujets de préoccupation pour la réputation de votre expéditeur.

> **Note**
>
> En ce qui concerne Outlook, elles couvrent tous les domaines suivis. Par exemple, elles peuvent couvrir Hotmail.com, Outlook.com et Live.com.

Pour afficher les données SNDS pour vos adresses IP dédiées

1. Connectez-vous à la console Amazon CloudWatch à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, développez Metrics (Métriques) et choisissez All metrics (Toutes les métriques).

   (Les instructions sont données pour la nouvelle interface de la console CloudWatch.)
3. Sous l'onglet Browse (Parcourir) dans le conteneur Metrics (Métriques), sélectionnez votre Région AWS, puis choisissez SES.
4. Choisissez IP Metrics (Métriques des adresses IP) pour afficher toutes vos adresses IP dédiées suivies par SNDS.

   (Remarque : si aucune adresse IP dédiée n'est associée à votre compte dans la région sélectionnée, IP Metrics (Métriques des adresses IP) n'apparaîtra pas dans la console CloudWatch.)
5. Affichez toutes vos adresses IP dédiées suivies par SPDN dans cette liste, ou sélectionnez une adresse IP spécifique pour afficher uniquement ses métriques.

Les métriques suivantes sont fournies pour chaque adresse IP dédiée et sont définies par Outlook. Pour plus d'informations, consultez la FAQ d'Outlook sur SNDS.

> **Note**
>
> Ces métriques représentent une période d'activité qui fournit des données mises à jour quotidiennement. Les métriques ont également un horodatage correspondant, qui reflète une période de 24 heures.

- SNDS.RCPTCommands - Il s'agit du nombre de commandes RCPT perçues par SNDS pour l'adresse IP spécifique au cours de la période d'activité. Les commandes RCPT font partie du

protocole SMTP utilisé pour envoyer des e-mails, qui spécifie l'adresse du destinataire à laquelle vous essayez de remettre l'e-mail.

- SNDS.DataCommands - Nombre de commandes DATA perçues par SNDS pour l'adresse IP spécifique au cours de la période d'activité. Les commandes DATA font partie du protocole SMTP utilisé pour envoyer des e-mails, en particulier la partie qui transmet en fait le message au(x) destinataire(s) prévu(s) préalablement établi(s).
- SNDS.MessageRecipients - Nombre de destinataires des messages perçus par SNDS pour l'adresse IP spécifique au cours de la période d'activité.
- SNDS.SpamRate - Affiche les résultats agrégés du filtrage du courrier indésirable appliqué à tous les messages envoyés par l'adresse IP pendant la période d'activité donnée.
  - Une valeur SpamRate de 0 signifie que l'adresse IP contient moins de 10 % de courrier indésirable.
  - Une valeur courrier SpamRate de 0,5 signifie qu'entre 10 % et 90 % de courrier indésirable est généré à partir de l'adresse IP.
  - Une valeur SpamRate de 1 signifie que 90 % ou plus de courrier indésirable est généré à partir de l'adresse IP.
- SNDS.ComplaintRate - Il s'agit de la fraction de temps pendant laquelle un message reçu par l'adresse IP fait l'objet d'une réclamation par un utilisateur Outlook au cours de la période d'activité.
  - Une valeur ComplaintRate de 1 correspond à un taux de réclamation de 100 %.
  - Une valeur ComplaintRate de 0,05 correspond à un taux de réclamation de 5 %, par exemple.
  - Une valeur ComplaintRate de 0 correspond à un taux inférieur à 0,1 %.
- SNDS.TrapHits - Affiche le nombre de messages envoyés aux « comptes d'interception ». Les comptes d'interception sont des comptes gérés par Outlook qui ne sollicitent aucun e-mail. Ainsi, tous les messages envoyés aux comptes d'interception sont très susceptibles d'être du courrier indésirable.

Questions relatives au dépannage

Q1. Pourquoi les données ne se remplissent-elles pas tous les jours ? L'un des scénarios suivants pourrait l'expliquer :

- Les données SNDS dépendent du programme SNDS d'Outlook.
- SNDS doit recevoir un seuil minimal d'e-mails pour calculer une valeur. Il se peut que les données ne soient pas disponibles lorsqu'une adresse IP contient peu d'e-mails.

Q2. Pourquoi les métriques SNDS.SpamRate et SNDS.ComplaintRate changent-elles, et que dois-je faire si le taux passe à 1 ?

Cela signifie que quelque chose dans votre comportement d'envoi a déclenché une réponse négative à partir du programme SNDS Outlook. Dans ce cas, vous devez vérifier les autres fournisseurs de services Internet (FAI) ainsi que vos numéros d'engagement pour vous assurer qu'il ne s'agit pas d'un problème général. S'il s'agit d'un problème général, vous pouvez voir des problèmes avec plusieurs FAI, ce qui suggère un problème de liste, de contenu, de distribution ou d'autorisations. Si le problème est spécifique à Outlook, consultez comment délivrer le plus efficacement à Outlook.

Q3. Quelles actions AWS Support prendra-t-il si la valeur de ma métrique SNDS.SpamRate passe de 0 (ou 0,5) à 1 ?

AWS n'a aucun contrôle, et donc aucune influence, sur SNDS. Toutes les demandes d'atténuation doivent être déposées directement auprès d'Outlook via le nouveau formulaire de demande de support.

Interruption automatique d'envoi d'e-mails

Pour protéger votre réputation d'expéditeur, vous pouvez temporairement suspendre l'envoi des messages envoyés à l'aide de jeux de configuration spécifiques ou de tous les messages envoyés depuis votre compte Amazon SES dans une région AWS spécifique.

En utilisant Amazon CloudWatch et Lambda, vous pouvez créer une solution qui suspend automatiquement votre envoi d'e-mails lorsque vos métriques de réputation (par exemple, taux de retour à l'expéditeur ou taux de réclamation) dépasse un seuil donné. Cette rubrique présente les procédures de configuration de cette solution.

Rubriques de cette section :

- Interruption automatique de l'envoi d'e-mails pour la totalité de votre compte Amazon SES
- Interruption automatique d'envoi d'e-mails pour un ensemble de configurations

Interruption automatique de l'envoi d'e-mails pour la totalité de votre compte Amazon SES

Les procédures de cette section expliquent comment configurer Amazon SES, Amazon SNS, Amazon CloudWatch et AWS Lambda de façon à suspendre automatiquement l'envoi d'e-mails

pour votre compte Amazon SES dans une seule région AWS. Si vous envoyez un e-mail à partir de plusieurs régions, répétez les procédures de cette section pour chaque région dans laquelle vous souhaitez mettre en œuvre cette solution.

Rubriques de cette section :

1ère partie : Création d'un rôle IAM

La première étape de la procédure de configuration de l'interruption automatique de l'envoi d'e-mails consiste à créer un rôle IAM capable de créer l'opération d'API `UpdateAccountSendingEnabled`.

Pour créer le rôle IAM

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Rôles.
3. Sélectionnez Create role (Créer un rôle).
4. Sur la page Select trusted entity (Sélectionner une entité de confiance), choisissez AWS service (Service AWS) pour Trusted entity type (Type d'entité de service).
5. Sous Use case (Cas d'utilisation), sélectionnez Lambda, puis Next (Suivant).
6. Sur la page Add permissions (Ajouter des autorisations), choisissez les stratégies suivantes :
   - AWSLambdaBasicExecutionRole
   - AmazonSESFullAccess

> **Tip**
>
> Utilisez la zone de recherche sous Permission policies (Politiques d'autorisation) pour localiser rapidement ces politiques, mais notez qu'après avoir recherché et sélectionné

la première politique, vous devez choisir Clear filters (Effacer les filtres) avant de rechercher et de sélectionner la deuxième politique.

Sélectionnez ensuite Next (Suivant).

7. Dans la page Name, review, and create (Nommer, vérifier et créer), sous Role details (Détails du rôle), entrez un nom significatif pour la politique dans le champ Role name (Nom du rôle).
8. Vérifiez que les deux politiques que vous avez sélectionnées sont répertoriées dans la table Permissions policy summary (Récapitulatif des politiques d'autorisation), puis choisissez Create role (Créer un rôle).

2e partie : Créer la fonction Lambda

Une fois que vous avez créé un rôle IAM, vous pouvez créer la fonction Lambda qui interrompt l'envoi d'e-mails pour votre compte.

Pour créer la fonction Lambda

1. Ouvrez la console AWS Lambda à l'adresse https://console.aws.amazon.com/lambda/.
2. Utilisez le sélecteur de région pour choisir la région dans laquelle vous souhaitez déployer la fonction Lambda.

   > **Note**
   >
   > Cette fonction interrompt l'envoi d'e-mails uniquement dans la région AWS sélectionnée au cours de cette étape. Si vous envoyez un e-mail à partir de plusieurs régions, répétez les procédures de cette section pour chaque région dans laquelle vous souhaitez interrompre automatiquement l'envoi d'e-mails.

3. Sélectionnez Create function (Créer une fonction).
4. Sous Create function (Créer une fonction), choisissez Author from scratch (Créer de bout en bout).
5. Sur la page Basic information (Informations de base), effectuez les étapes suivantes :

   - Pour Function name (Nom de la fonction), attribuez un nom à la fonction Lambda.
   - Pour Environnement d'exécution, choisissez Node.js 18x (ou la version actuellement proposée dans la liste de sélection).

- Pour Architecture, conservez la valeur par défaut présélectionnée, x86_64.
- Sous Permissions (Autorisations), développez Change default execution role (Modifier le rôle d'exécution par défaut) et choisissez Use an existing role (Utiliser un rôle existant).
- Cliquez à l'intérieur de la liste déroulante Existing role (Rôle existant) et choisissez le rôle IAM que vous avez créé dans the section called “1ère partie : Création d'un rôle IAM”.

Puis, choisissez Créer une fonction.

6. Sous Code source (Source de code), dans l'éditeur de code, collez le code suivant :

```
'use strict';


const { SES } = require("@aws-sdk/client-ses")

// Create a new SES object.

var ses = new SES({});

// Specify the parameters for this operation. In this case, there is only one
// parameter to pass: the Enabled parameter, with a value of false
// (Enabled = false disables email sending, Enabled = true enables it).
var params = {
    Enabled: false
};

exports.handler = (event, context, callback) => {
    // Pause sending for your entire SES account
    ses.updateAccountSendingEnabled(params, function(err, data) {
        if(err) {
            console.log(err.message);
        } else {
            console.log(data);
        }
    });
};
```

Choisissez ensuite Deploy (Déployer).

7. Choisissez Test (Tester). Si la fenêtre Configure test event (Configurer un événement de test) s'affiche, entrez un nom dans le champ Event name (Nom d'événement), puis choisissez Save (Enregistrer).
8. Développer la zone déroulante Test et sélectionnez le nom de l'événement que vous venez de créer, puis choisissez Test.
9. L'onglet Execution results (Résultats de l'exécution) apparaîtra, juste en dessous et à droite, assurez-vous que `Status: Succeeded` s'affiche. Si la fonction n'a pas pu s'exécuter, procédez comme suit :

   - Vérifiez que le rôle IAM que vous avez créé dans la the section called "1ère partie : Création d'un rôle IAM" contient les stratégies appropriées.
   - Vérifiez que le code de la fonction Lambda ne comporte pas d'erreurs. L'éditeur de code Lambda met automatiquement en surbrillance les erreurs de syntaxe et d'autres problèmes potentiels.

3e partie : Réactivation de l'envoi d'e-mails pour votre compte

Le test de la fonction Lambda dans la the section called "2e partie : Créer la fonction Lambda" a pour conséquence d'interrompre l'envoi d'e-mails pour votre compte Amazon SES. Dans la plupart des cas, il n'y a aucun intérêt à interrompre l'envoi pour votre compte du moment que l'alarme CloudWatch n'est pas déclenchée.

Les procédures de cette section visent à réactiver l'envoi d'e-mails pour votre compte Amazon SES. Pour effectuer ces procédures, vous devez installer et configurer l' AWS Command Line Interface. Pour en savoir plus, veuillez consulter le Guide de l'utilisateur AWS Command Line Interface.

Pour réactiver l'envoi d'e-mails

1. Sur la ligne de commande, entrez la commande suivante pour réactiver l'envoi d'e-mails pour votre compte. Remplacez *`sending_region`* par le nom de la région dans laquelle vous souhaitez réactiver l'envoi d'e-mails.

   ```
   aws ses update-account-sending-enabled --enabled --region sending_region
   ```

2. Sur la ligne de commande, entrez la commande suivante pour vérifier le statut d'envoi d'e-mails pour votre compte :

```
aws ses get-account-sending-enabled --region sending_region
```

Si vous voyez la sortie suivante, c'est que vous avez réussi à réactiver l'envoi d'e-mails pour votre compte :

```
{
    "Enabled": true
}
```

4e partie : Créer une rubrique Amazon SNS et s'abonner

Pour que CloudWatch exécute votre fonction Lambda lors du déclenchement d'une alarme, vous devez d'abord créer une rubrique Amazon SNS et abonner la fonction Lambda à cette dernière.

Pour créer une rubrique Amazon SNS et y abonner la fonction Lambda

1. Ouvrez la console Amazon SNS à partir de l'adresse https://console.aws.amazon.com/sns/v3/home.
2. Créez une rubrique en suivant les étapes décrites dans le Guide du développeur Amazon Simple Notification Service.
   - Le Type doit être Standard (et non FIFO).
3. Abonnez-vous à la rubrique en suivant les étapes décrites dans le Guide du développeur Amazon Simple Notification Service.
   a. Pour Protocole, choisissez AWS Lambda.
   b. Pour Endpoint (Point de terminaison), choisissez la fonction Lambda que vous avez créée dans la the section called “2e partie : Créer la fonction Lambda”.

5e partie : Création d'une alarme CloudWatch

Cette section contient des procédures visant à créer une alarme dans CloudWatch qui se déclenche lorsqu'une métrique atteint un certain seuil. Lorsqu'elle se déclenche, l'alarme adresse une notification à la rubrique Amazon SNS que vous avez créée dans la the section called “4e partie : Créer une rubrique Amazon SNS et s'abonner”, qui exécute alors la fonction Lambda que vous avez créée dans la the section called “2e partie : Créer la fonction Lambda”.

Pour créer une alarme CloudWatch

1. Ouvrez la console CloudWatch à l'adresse https://console.aws.amazon.com/ CloudWatch/.
2. Utilisez le sélecteur de région pour choisir la région dans laquelle vous souhaitez interrompre automatiquement l'envoi d'e-mails.
3. Dans le panneau de navigation, cliquez sur Alarms (Alarmes).
4. Sélectionnez Create Alarm (Créer une alarme).
5. Dans la fenêtre Create Alarm (Créer une alarme), sous SES Metrics (Métriques SES), choisissez Account Metrics (Métriques du compte).
6. Sous Metric Name (Nom de la métrique), choisissez l'une des options suivantes :

   - Reputation.BounceRate – Choisissez cette métrique si vous souhaitez interrompre l'envoi d'e-mails pour votre compte du moment où le taux de messages d'erreur définitifs de votre compte franchit un seuil que vous définissez.
   - Reputation.ComplaintRate – Choisissez cette métrique si vous souhaitez interrompre l'envoi d'e-mails pour votre compte du moment où le taux de réclamations global de votre compte franchit un seuil que vous définissez.

   Choisissez Next (Suivant).
7. Procédez comme suit :

   - Sous Alarm Threshold (Seuil d'alarme), pour Name (Nom), saisissez un nom pour l'alarme.
   - Sous Whenever: Reputation.BounceRate (Chaque fois que : Reputation.BounceRate) ou Whenever: Reputation.ComplaintRate (Chaque fois que : Reputation.ComplaintRate), spécifiez le seuil qui déclenche l'alarme.

     > **Note**
     >
     > Votre compte est placé automatiquement sous vérification si votre taux de retours à l'expéditeur dépasse 10 % ou si votre taux de réclamations dépasse 0,5 %. Lorsque vous spécifiez le taux de retours à l'expéditeur ou le taux de réclamations qui déclenche l'alarme CloudWatch, nous vous recommandons d'utiliser des valeurs inférieures à ces taux pour empêcher la mise sous vérification de votre compte.

   - Sous Actions, pour Whenever this alarm (Chaque fois que cette alarme), choisissez State is ALARM (l'état est ALARME). Pour Send notification to (Envoyer la notification à), choisissez la

rubrique Amazon SNS que vous avez créée dans la the section called “4e partie : Créer une rubrique Amazon SNS et s'abonner”.

Choisissez Create Alarm (Créer l'alarme).

6e partie : Test de la solution

Vous pouvez maintenant tester l'alarme afin de vérifier qu'elle exécute la fonction Lambda lorsqu'elle passe à l'état `ALARM`. Vous pouvez utiliser l'opération d'API `SetAlarmState` pour modifier temporairement l'état de l'alarme.

Bien que les procédures de cette section soient facultatives, nous vous recommandons de les exécuter pour vérifier que l'ensemble de la solution est correctement configurée.

1. Sur la ligne de commande, entrez la commande suivante pour vérifier le statut d'envoi d'e-mails pour votre compte. Remplacez *`region`* par le nom de la région.

   ```
   aws ses get-account-sending-enabled --region region
   ```

   Si l'envoi est activé pour votre compte, vous obtenez la sortie suivante :

   ```
   {
       "Enabled": true
   }
   ```

2. Sur la ligne de commande, tapez la commande suivante afin de changer temporairement l'état de l'alarme en `ALARM` : aws cloudwatch set-alarm-state --alarm-name ***`MyAlarm`*** --state-value ALARM --state-reason "Testing execution of Lambda function" --region ***`region`***

   Dans la commande précédente, remplacez *`MyAlarm`* par le nom de l'alarme que vous avez créée dans the section called “5e partie : Création d'une alarme CloudWatch” et remplacez *`region`* par la région dans laquelle vous souhaitez interrompre automatiquement l'envoi d'e-mails.

   > **Note**
   >
   > Lorsque vous exécutez cette commande, le statut de l'alarme passe de `OK` à `ALARM` et de nouveau à `OK` en l'espace de quelques secondes. Vous pouvez examiner ces

changements de statut dans l'onglet History (Historique) de l'alarme dans la console CloudWatch ou en utilisant l'opération DescribeAlarmHistory.

3. Sur la ligne de commande, entrez la commande suivante pour vérifier le statut d'envoi d'e-mails pour votre compte.

```
aws ses get-account-sending-enabled --region region
```

Si la fonction Lambda a été exécutée correctement, vous obtenez la sortie suivante :

```
{
    "Enabled": false
}
```

4. Effectuez les étapes de la the section called “3e partie : Réactivation de l'envoi d'e-mails pour votre compte” pour réactiver l'envoi d'e-mails pour votre compte.

Interruption automatique d'envoi d'e-mails pour un ensemble de configurations

Vous pouvez configurer Amazon SES pour exporter des métriques de réputation spécifiques à des e-mails envoyés à l'aide d'un jeu de configurations donné vers Amazon CloudWatch. Vous pouvez ensuite utiliser ces métriques pour créer des alarmes CloudWatch spécifiques à ces jeux de configurations. Lorsque ces alarmes dépassent un certain seuil, vous pouvez automatiquement interrompre l'envoi d'e-mails qui utilisent les jeux de configurations spécifiés, sans aucune répercussion sur les capacités globales d'envoi d'e-mails de votre compte Amazon SES.

> **Note**
>
> La solution décrite dans cette section interrompt l'envoi d'e-mails pour un jeu de configurations spécifique dans une seule région AWS. Si vous envoyez un e-mail à partir de plusieurs régions, répétez les procédures de cette section pour chaque région dans laquelle vous souhaitez mettre en œuvre cette solution.

Rubriques de cette section :

1ère partie : Activation de la génération de rapports de métriques de réputation pour l'ensemble de configurations

Avant de pouvoir configurer l'interruption automatique de l'envoi d'e-mails pour un jeu de configurations dans Amazon SES, vous devez d'abord activer l'exportation des métriques de réputation pour le jeu de configurations.

Pour activer l'exportation de métriques de retour à l'expéditeur et de réclamation pour l'ensemble de configurations, complétez les étapes détaillées dans the section called “Afficher et exporter des mesures de réputation”.

2e partie : Création d'un rôle IAM

La première étape de la procédure de configuration de l'interruption automatique de l'envoi d'e-mails consiste à créer un rôle IAM capable de créer l'opération d'API `UpdateConfigurationSetSendingEnabled`.

Pour créer le rôle IAM

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Rôles.
3. Sélectionnez Create role (Créer un rôle).
4. Sous Select type of trusted entity (Sélectionner le type d'entité approuvée), choisissez service AWS.
5. Sous Choose the service that will use this role (Choisir le service qui utilisera ce rôle), choisissez Lambda. Sélectionnez Next: Permissions (Étape suivante : autorisations).

6. Sur la page Attach permissions policies (Attacher les stratégies d'autorisations), choisissez les stratégies suivantes :

   - AWS LambdaBasicExecutionRole
   - AmazonSESFullAccess

   > **Tip**
   >
   > Pour accéder rapidement à ces stratégies, servez-vous de la zone de recherche située en haut de la liste des stratégies.

   Choisissez Next: Review (Suivant : Vérification).

7. Sur la page Review (Vérifier), dans Name (Nom), attribuez un nom au rôle. Sélectionnez Create role (Créer un rôle).

3e partie : Création de la fonction Lambda

Une fois que vous avez créé un rôle IAM, vous pouvez créer la fonction Lambda qui interrompt l'envoi d'e-mails pour le jeu de configurations.

Pour créer la fonction Lambda

1. Ouvrez la console AWS Lambda à l'adresse https://console.aws.amazon.com/lambda/.
2. Utilisez le sélecteur de région pour choisir la région dans laquelle vous souhaitez déployer la fonction Lambda.

   > **Note**
   >
   > Cette fonction interrompt l'envoi d'e-mails uniquement pour les jeux de configurations de la région AWS sélectionnée au cours de cette étape. Si vous envoyez un e-mail à partir de plusieurs régions, répétez les procédures de cette section pour chaque région dans laquelle vous souhaitez interrompre automatiquement l'envoi d'e-mails.

3. Sélectionnez Create function (Créer une fonction).

4. Sous Create function (Créer une fonction), choisissez Author from scratch (Créer de bout en bout).
5. Sous Author from scratch (Créer de bout en bout), procédez comme suit :

   - Pour Name (Nom), attribuez un nom à la fonction Lambda.
   - Pour Runtime (Exécution), choisissez Node.js 14 (ou la version actuellement proposée dans la liste de sélection).
   - Pour Role (Rôle), choisissez Choose an existing role (Sélectionner un rôle existant).
   - Pour Existing role (Rôle existant), choisissez le rôle IAM que vous avez créé dans the section called “2e partie : Création d'un rôle IAM”.

   Sélectionnez Create function (Créer une fonction).
6. Sous Function code (Code de fonction), dans l'éditeur de code, collez le code suivant :

```
'use strict';

var aws = require('aws-sdk');

// Create a new SES object.
var ses = new aws.SES();

// Specify the parameters for this operation. In this example, you pass the
// Enabled parameter, with a value of false (Enabled = false disables email
// sending, Enabled = true enables it). You also pass the ConfigurationSetName
// parameter, with a value equal to the name of the configuration set for
// which you want to pause email sending.
var params = {
    ConfigurationSetName: ConfigSet,
    Enabled: false
};

exports.handler = (event, context, callback) => {
    // Pause sending for a configuration set
    ses.updateConfigurationSetSendingEnabled(params, function(err, data) {
        if(err) {
            console.log(err.message);
        } else {
            console.log(data);
        }
    });
```

```
};
```

Dans le code précédent, remplacez *ConfigSet* par le nom de l'ensemble de configurations. Choisissez Save (Enregistrer).

7. Sélectionnez Test (Tester). Si la fenêtre Configure test event (Configurer un événement de test) s'affiche, entrez un nom dans le champ Event name (Nom d'événement), puis choisissez Create (Créer).
8. Vérifiez que la barre de notifications située en haut de la page indique bien `Execution result: succeeded`. Si la fonction n'a pas pu s'exécuter, procédez comme suit :

   - Vérifiez que le rôle IAM que vous avez créé dans la the section called “2e partie : Création d'un rôle IAM” contient les stratégies appropriées.
   - Vérifiez que le code de la fonction Lambda ne comporte pas d'erreurs. L'éditeur de code Lambda met automatiquement en surbrillance les erreurs de syntaxe et d'autres problèmes potentiels.

4e partie : Réactivation de l'envoi d'e-mails pour l'ensemble de configurations

Le test de la fonction Lambda dans la the section called “3e partie : Création de la fonction Lambda” a pour conséquence d'interrompre l'envoi d'e-mails pour le jeu de configurations. Dans la plupart des cas, vous ne souhaitez pas interrompre l'envoi pour le jeu de configurations tant que l'alarme CloudWatch n'est pas déclenchée.

Les procédures de cette section visent à réactiver l'envoi d'e-mails pour votre ensemble de configurations. Pour effectuer ces procédures, vous devez installer et configurer l' AWS Command Line Interface. Pour en savoir plus, veuillez consulter le Guide de l'utilisateur AWS Command Line Interface.

Pour réactiver l'envoi d'e-mails

1. Sur la ligne de commande, entrez la commande suivante pour réactiver l'envoi d'e-mails pour l'ensemble de configurations :

```
aws ses update-configuration-set-sending-enabled \
--configuration-set-name ConfigSet \
--enabled
```

Dans la commande précédente, remplacez *ConfigSet* par le nom du jeu de configurations pour lequel vous souhaitez interrompre l'envoi d'e-mails.

2. Sur la ligne de commande, entrez la commande suivante pour vérifier que l'envoi d'e-mails est activé :

```
aws ses describe-configuration-set \
--configuration-set-name ConfigSet \
--configuration-set-attribute-names reputationOptions
```

Cette commande produit un résultat similaire à ce qui suit :

```
{
    "ConfigurationSet": {
        "Name": "ConfigSet"
    },
    "ReputationOptions": {
        "ReputationMetricsEnabled": true,
        "SendingEnabled": true
    }
}
```

Si la valeur de `SendingEnabled` est `true`, l'envoi d'e-mails pour l'ensemble de configurations a été correctement réactivé.

5e partie : Créer une rubrique Amazon SNS

Pour que CloudWatch exécute la fonction Lambda lors du déclenchement d'une alarme, vous devez d'abord créer une rubrique Amazon SNS et abonner la fonction Lambda à cette dernière.

Pour créer la rubrique Amazon SNS

1. Ouvrez la console Amazon SNS à partir de l'adresse https://console.aws.amazon.com/sns/v3/home.
2. Utilisez le sélecteur de région pour choisir la région dans laquelle vous souhaitez interrompre automatiquement l'envoi d'e-mails.
3. Dans le panneau de navigation, sélectionnez Topics (Rubriques).
4. Choisissez Create new topic (Créer une nouvelle rubrique).

5. Dans la fenêtre Create new topic (Créer une nouvelle rubrique), dans Topic name (Nom de rubrique), attribuez un nom à la rubrique. Si vous le souhaitez, vous pouvez entrer un nom plus descriptif dans le champ Display name (Nom d'affichage).

   Choisissez Create topic (Créer une rubrique).
6. Dans la liste des rubriques, cochez la case en regard de la rubrique que vous avez créée à l'étape précédente. Dans le menu Actions, choisissez Subscribe to topic (S'abonner à la rubrique).
7. Dans la fenêtre Create subscription (Créer un abonnement), effectuez les sélections suivantes :

   - Pour Protocol (Protocole), choisissez AWS Lambda.
   - Pour Endpoint (Point de terminaison), choisissez la fonction Lambda que vous avez créée dans la the section called “3e partie : Création de la fonction Lambda”.
   - Pour Version or alias (Version ou alias), choisissez default (par défaut).
8. Choisissez Create subscription (Créer un abonnement).

6e partie : Pour créer une alarme CloudWatch

Cette section contient des procédures visant à créer une alarme dans CloudWatch qui se déclenche lorsqu'une métrique atteint un certain seuil. Lorsqu'elle se déclenche, l'alarme adresse une notification à la rubrique Amazon SNS que vous avez créée dans la the section called “5e partie : Créer une rubrique Amazon SNS”, qui exécute alors la fonction Lambda que vous avez créée dans la the section called “3e partie : Création de la fonction Lambda”.

Pour créer une alarme CloudWatch

1. Ouvrez la console CloudWatch à l'adresse https://console.aws.amazon.com/ CloudWatch/.
2. Utilisez le sélecteur de région pour choisir la région dans laquelle vous souhaitez interrompre automatiquement l'envoi d'e-mails.
3. Dans le panneau de navigation de gauche, choisissez Alarms (Alarmes).
4. Sélectionnez Create Alarm (Créer une alarme).
5. Dans la fenêtre Create Alarm (Créer une alarme), sous SES Metrics (Métriques SES), choisissez Configuration Set Metrics (Métriques de l'ensemble de configurations).
6. Dans la colonne ses:configuration-set, identifiez l'ensemble de configurations pour lequel vous souhaitez créer une alarme. Sous Metric Name (Nom de la métrique), choisissez l'une des options suivantes :

- Reputation.BounceRate – Choisissez cette métrique si vous souhaitez interrompre l'envoi d'e-mails pour l'ensemble de configurations dès lors que le taux global de messages d'erreur définitifs pour l'ensemble de configurations franchit un seuil que vous définissez.
- Reputation.ComplaintRate – Choisissez cette métrique si vous souhaitez interrompre l'envoi d'e-mails pour l'ensemble de configurations dès lors que le taux global de réclamations pour l'ensemble de configurations franchit un seuil que vous définissez.

Choisissez Next (Suivant).

7. Procédez comme suit :

- Sous Alarm Threshold (Seuil d'alarme), pour Name (Nom), saisissez un nom pour l'alarme.
- Sous Whenever: Reputation.BounceRate (Chaque fois que : Reputation.BounceRate) ou Whenever: Reputation.ComplaintRate (Chaque fois que : Reputation.ComplaintRate), spécifiez le seuil qui déclenche l'alarme.

> **Note**
>
> Si le taux global de retours à l'expéditeur pour votre compte Amazon SES dépasse 10 %, ou si le taux global de réclamations pour votre compte Amazon SES dépasse 0,5 %, votre compte Amazon SES est automatiquement placé sous vérification. Lorsque vous spécifiez le taux de retour à l'expéditeur ou le taux de réclamation qui déclenche l'alarme CloudWatch, nous vous recommandons d'utiliser des valeurs bien inférieures à ces taux pour empêcher la mise sous vérification de votre compte.

- Sous Actions, pour Whenever this alarm (Chaque fois que cette alarme), choisissez State is ALARM (L'état est ALARME). Pour Send notification to (Envoyer la notification à), choisissez la rubrique Amazon SNS que vous avez créée dans la the section called “5e partie : Créer une rubrique Amazon SNS”.

Choisissez Create Alarm (Créer l'alarme).

7e partie : Test de la solution

Vous pouvez maintenant tester l'alarme afin de vérifier qu'elle exécute la fonction Lambda lorsqu'elle passe à l'état `ALARM`. Vous pouvez utiliser l'opération `SetAlarmState` dans l'API CloudWatch pour modifier temporairement l'état de l'alarme.

Bien que les procédures de cette section soient facultatives, nous vous recommandons de les exécuter pour vérifier que l'ensemble de la solution est correctement configurée.

Pour tester la solution

1. Sur la ligne de commande, entrez la commande suivante pour vérifier le statut d'envoi d'e-mails pour l'ensemble de configurations :

   ```
   aws ses describe-configuration-set --configuration-set-name ConfigSet
   ```

   Si l'envoi est activé pour l'ensemble de configurations défini, vous voyez la sortie suivante :

   ```
   {
       "ConfigurationSet": {
           "Name": "ConfigSet"
       },
       "ReputationOptions": {
           "ReputationMetricsEnabled": true,
           "SendingEnabled": true
       }
   }
   ```

   Si la valeur de `SendingEnabled` est `true`, l'envoi d'e-mails pour l'ensemble de configurations est activé.
2. Sur la ligne de commande, entrez la commande suivante afin de changer temporairement l'état de l'alarme en `ALARM` :

   ```
   aws cloudwatch set-alarm-state \
   --alarm-name MyAlarm \
   --state-value ALARM \
   --state-reason "Testing execution of Lambda function"
   ```

   Dans la commande précédente, remplacez *MyAlarm* par le nom de l'alarme que vous avez créée dans la the section called “6e partie : Pour créer une alarme CloudWatch”.

> **Note**
>
> Lorsque vous exécutez cette commande, le statut de l'alarme passe de `OK` à `ALARM` et de nouveau à `OK` en l'espace de quelques secondes. Vous pouvez examiner ces changements de statut dans l'onglet History (Historique) de l'alarme dans la console CloudWatch ou en utilisant l'opération DescribeAlarmHistory.

3. Sur la ligne de commande, entrez la commande suivante pour vérifier le statut d'envoi d'e-mails pour l'ensemble de configurations :

```
aws ses describe-configuration-set \
--configuration-set-name ConfigSet
```

Si la fonction Lambda est exécutée avec succès, vous obtiendrez une sortie similaire à l'exemple suivant :

```
{
    "ConfigurationSet": {
        "Name": "ConfigSet"
    },
    "ReputationOptions": {
        "ReputationMetricsEnabled": true,
        "SendingEnabled": false
    }
}
```

Si la valeur de `SendingEnabled` est `false`, l'envoi d'e-mails pour le jeu de configurations est désactivé, indiquant que la fonction Lambda a été exécutée avec succès.

4. Suivez les étapes de the section called “4e partie : Réactivation de l'envoi d'e-mails pour l'ensemble de configurations” pour réactiver l'envoi d'e-mails pour l'ensemble de configurations.

Surveillance des événements SES à l'aide d'Amazon EventBridge

EventBridge est un service sans serveur qui utilise des événements pour connecter les composants de l'application entre eux, ce qui vous permet de créer plus facilement des applications évolutives pilotées par des événements. L'architecture axée sur les événements est un style de création de systèmes logiciels à couplage faible qui fonctionnent ensemble en émettant des événements et en y répondant. Les événements sont des messages au format JSON qui représentent généralement une modification d'une ressource ou d'un environnement, ou un autre événement de gestion.

Certaines fonctionnalités de SES génèrent et envoient des événements au bus d'événements EventBridge par défaut. Un bus d'événements est un routeur qui reçoit des événements et les transmet à zéro ou plusieurs destinations, ou cibles. Les règles que vous associez au bus d'événements évaluent les événements au fur et à mesure qu'ils arrivent. Chaque règle vérifie si un événement correspond au modèle de la règle. Si l'événement correspond, EventBridge envoie l'événement aux cibles spécifiées.

SES envoie des événements en EventBridge cas de changement d'état ou de mise à jour de statut d'une fonctionnalité. Vous pouvez utiliser des EventBridge règles pour acheminer les événements vers les cibles que vous avez définies. Ces événements seront transmis dans la mesure du possible, et il se peut qu'ils ne soient pas transmis dans l'ordre.

Rubriques

Événements SES

Les événements suivants sont générés par les fonctionnalités de SES et envoyés au bus d'événements par défaut dans EventBridge. Pour plus d'informations, y compris les données détaillées pour chaque type d'événement, consultez???.

Événements destinés aux conseillers de Virtual Deliverability Manager

Type d’événement	Description
Statut de recommandation du conseiller ouvert	Un événement généré chaque fois qu'une nouvelle recommandation est ouverte dans le conseiller du gestionnaire de délivrabilité virtuel.
Statut de recommandation du conseiller résolu	Un événement généré chaque fois qu'une recommandation est résolue dans le conseiller du gestionnaire de délivrabilité virtuel.

Événements d'envoi d'e-mails SES

Type d’événement	Description
E-mail renvoyé	Un hard bounce indiquant que le serveur de messagerie du destinataire a définitivement rejeté l'e-mail. Les messages d'erreur temporaires sont inclus uniquement quand SES ne parvient pas à remettre l'e-mail après plusieurs tentatives au cours d'une période donnée.
E-mail cliqué	Le destinataire a cliqué sur un ou plusieurs liens contenus dans l'e-mail.
Réception d'une plainte par e-mail	L'e-mail a bien été envoyé au serveur de messagerie du destinataire, mais celui-ci l'a marqué comme spam.
Livraison d'e-mail	SES a correctement envoyé l'e-mail au serveur de messagerie du destinataire.
Livraison du courrier électronique retardée	L'e-mail n'a pas pu être remis au serveur de messagerie du destinataire en raison d'un problème temporaire. Des retards de livraison peuvent se produire, par exemple lorsque la boîte de réception du destinataire est pleine ou lorsque le serveur de messagerie de réception rencontre un problème transitoire.
Courrier électronique ouvert	Le destinataire a reçu le message et l'a ouvert dans son client de messagerie.

Type d'événement	Description
E-mail refusé	SES a accepté l'e-mail, mais a déterminé qu'il contenait un virus et n'a pas tenté de le transmettre au serveur de messagerie du destinataire.
Échec du rendu de l'e-mail	L'e-mail n'a pas été envoyé en raison d'un problème de rendu du modèle. Ce type d'événement peut se produire lorsqu'il manque des données du modèle ou lorsqu'il n'y a pas concordance entre les paramètres du modèle et les données. Ce type d'événeme nt ne se produit que lorsque vous envoyez un e-mail à l'aide des opérations d'API `SendTemplatedEmail` ou `SendBulkTemplatedEmail`.
Courrier électronique envoyé	La demande d'envoi a réussi et SES tentera de remettre le message au serveur de messagerie du destinataire. (Si une suppression globale ou au niveau du compte est utilisée, SES la comptera toujours comme un envoi, mais la livraison sera supprimée).
Adresse e-mail souscrite	L'e-mail a été envoyé avec succès, mais le destinataire a mis à jour les préférences d'abonnement en cliquant `List-Unsubscribe` dans l'en-tête de l'e-mail ou sur le `Unsubscribe` lien dans le pied de page.

Référence du schéma des événements SES

Tous les événements issus AWS des services ont un ensemble commun de champs contenant des métadonnées relatives à l'événement, telles que le AWS service à l'origine de l'événement, l'heure à laquelle l'événement a été généré, le compte et la région dans lesquels l'événement a eu lieu, etc. Pour les définitions de ces champs généraux, voir la référence relative à la structure des événements dans le guide de EventBridge l'utilisateur.

En outre, chaque événement possède un champ `detail` qui contient des données spécifiques à cet événement en particulier. La référence ci-dessous définit les champs détaillés des différents événements SES.

Lorsque vous EventBridge les utilisez pour sélectionner et gérer des événements SES, il est utile de garder à l'esprit les points suivants :

- Le champ `source` pour tous les événements de SES est défini sur `aws.ses`.
- Le champ `detail-type` indique le type d'événement. Consultez le tableau des types d'événements dansthe section called “Événements SES”.
- Le champ `detail` contient les données spécifiques à cet événement en particulier.

  Pour certains types d'événements, tels que ceux de Virtual Deliverability Manager, le champ de détail est une chaîne de données plutôt simpliste remplie à partir d'un ensemble fini de valeurs statiques. À l'inverse, le champ de détail des événements d'envoi d'e-mails est plus complexe car il peut être composé de nombreux sous-champs de détail combinant des valeurs statiques et dynamiques, telles que l'horodatage de l'envoi d'un e-mail, l'adresse du destinataire et de nombreux autres attributs du courrier électronique.

Rubriques

Schéma de statut du conseiller du gestionnaire de délivrabilité virtuel

La référence de schéma suivante définit les champs spécifiques aux événements relatifs au statut des conseillers de Virtual Deliverability Manager.

Les définitions des champs généraux qui apparaissent dans tous les schémas d'événements (tels que`version`,, `idaccount`, et autres) se trouvent dans la section Référence de la structure des événements dans le guide de l'EventBridge utilisateur. Les champs `source` et `detail-type` sont inclus dans la référence ci-dessous, car ils contiennent des valeurs spécifiques à SES pour les événements SES.

`source`

Identifie le service qui a généré l'événement. Pour les événements SES, cette valeur est `aws.ses`.

`detail-type`

Identifie le type d'événement.

Les valeurs de ce champ sont répertoriées dans le tableau des événements du conseiller Virtual Deliverability Manager dansthe section called “Événements SES”.

`detail`

Un objet JSON qui contient des informations sur l'événement. Le service qui génère l'événement détermine le contenu de ce champ.

Les valeurs de ce champ peuvent être les suivantes :

- `DKIM verification is not enabled.`
- `DKIM verification has failed.`
- `DKIM signing key length is below 2048 bits.`
- `DMARC configuration was not found.`
- `DMARC configuration could not be parsed.`
- `DKIM record was not found.`
- `DKIM record is not aligned.`
- `MAIL FROM record is not aligned.`
- `SPF record was not found.`
- `SPF record for Amazon SES was not found.`
- `SPF all qualifier is missing.`
- `An SPF configuration issue was found.`
- `BIMI record not found or configured without default selector.`
- `BIMI has malformed TXT record.`

Example Exemple : événement de statut du conseiller du gestionnaire de délivrabilité virtuel

Voici un exemple d'événement de statut du conseiller du gestionnaire de délivrabilité virtuel pour ce type d'événement `Advisor Recommendation Status Open`. La valeur de l'événement détaillé dans cet exemple est`SPF record was not found.`.

```
{
 "version": "0",
  "id": "abcd9999-ef33-0123-90ab-abcdef666666",
  "detail-type": "Advisor Recommendation Status Open",
  "source": "aws.ses",
```

```
  "account": "012345678901",
  "time": "2023-11-15T17:00:59Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ses:us-east-1:012345678901:identity/vdm.events-publishing.cajun.syster-
games.example.com"
  ],
  "detail": { "version": "1.0.0", "data": "SPF record was not found." }
}
```

Schéma d'état d'envoi d'e-mails SES

La référence de schéma suivante définit les champs spécifiques aux événements de statut d'envoi d'e-mails SES.

Les définitions des champs généraux qui apparaissent dans tous les schémas d'événements (tels que`version`,, `idaccount`, et autres) se trouvent dans la section Référence de la structure des événements dans le guide de l'EventBridge utilisateur. Les champs `source` et `detail-type` sont inclus dans la référence ci-dessous, car ils contiennent des valeurs spécifiques à SES pour les événements SES.

`source`

Identifie le service qui a généré l'événement. Pour les événements SES, cette valeur est `aws.ses`.

`detail-type`

Identifie le type d'événement.

Les valeurs de ce champ sont répertoriées dans le tableau des événements d'envoi d'e-mails SES dansthe section called “Événements SES”.

`detail`

Un objet JSON qui contient des informations sur l'événement. Le service qui génère l'événement détermine le contenu de ce champ.

Toutes les valeurs possibles pour ce champ ne peuvent pas être répertoriées ici car elles sont composées de valeurs statiques et dynamiques générées par chaque e-mail unique envoyé à un moment donné. Cependant, un exemple est fourni pour vous donner une idée du type de données que ce champ peut contenir. Des exemples de données détaillées pour tous les

types d'événements d'envoi d'e-mails peuvent être trouvés à l'aide de la EventBridge Sandbox, voirSpécifiez un exemple d'événement dans EventBridge.

Voici un exemple de données détaillées générées pour l'événement d'envoi d'e-mails de SES `Email Rendering Failed` :

```
...,
  "detail": {
    "eventType": "Rendering Failure",
    "mail": {
      "timestamp": "2018-01-22T18:43:06.197Z",
      "source": "sender@example.com",
      "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
      "sendingAccountId": "123456789012",
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "destination": ["recipient@example.com"],
      "headersTruncated": false,
      "tags": {
        "ses:configuration-set": ["ConfigSet"]
      }
    },
    "failure": {
      "errorMessage": "Attribute 'attributeName' is not present in the rendering
 data.",
      "templateName": "MyTemplate"
    }
  }
```

Example Exemple : événement relatif au statut d'envoi d'un e-mail

Voici un exemple de l'événement complet relatif au statut d'envoi d'un e-mail pour le type d'événement`Email Rendering Failed`. Dans cet exemple, la valeur détaillée de l'événement est une combinaison de valeurs statiques et dynamiques basée sur l'événement d'envoi d'un e-mail spécifique.

```
{
  "version": "0",
  "id": "12a18625-3328-fafd-2809-a5e16004f112",
  "detail-type": "Email Rendering Failed",
  "source": "aws.ses",
  "account": "123456789012",
```

```
  "time": "2023-07-17T16:48:05Z",
  "region": "us-east-1",
  "resources": ["arn:aws:ses:us-east-1:123456789012:identity/example.com"],
  "detail": {
    "eventType": "Rendering Failure",
    "mail": {
      "timestamp": "2018-01-22T18:43:06.197Z",
      "source": "sender@example.com",
      "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
      "sendingAccountId": "123456789012",
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "destination": ["recipient@example.com"],
      "headersTruncated": false,
      "tags": {
        "ses:configuration-set": ["ConfigSet"]
      }
    },
    "failure": {
      "errorMessage": "Attribute 'attributeName' is not present in the rendering
 data.",
      "templateName": "MyTemplate"
    }
  }
}
```

Utilisation EventBridge avec des événements SES

Par défaut, SES envoie les événements au bus d'événements EventBridge par défaut. Vous pouvez créer des règles sur le bus d'événements par défaut afin d'identifier des événements spécifiques EventBridge à envoyer à une ou plusieurs cibles spécifiées. Chaque règle contient un modèle d'événement qui permet EventBridge de faire correspondre les événements lorsqu'ils arrivent sur le bus d'événements. Si un événement correspond au modèle d'événement d'une règle donnée, EventBridge envoie l'événement à la cible spécifiée dans la règle.

Dans EventBridge, la définition d'un modèle d'événement fait généralement partie du processus plus large de création d'une nouvelle règle ou de modification d'une règle existante. Pour savoir comment créer des EventBridge règles, consultez la section Création de EventBridge règles Amazon qui réagissent aux événements dans le Guide de EventBridge l'utilisateur.

À l'aide de la fonctionnalité Sandbox EventBridge, vous pouvez définir rapidement un modèle d'événement et utiliser un exemple d'événement pour confirmer que le modèle correspond aux

événements souhaités, sans avoir à créer ou à modifier une règle au préalable. Pour obtenir des instructions détaillées sur l'utilisation du Sandbox, voir Tester un modèle d'événement à l'aide du EventBridge Sandbox dans le Guide de l'EventBridge utilisateur.

Spécifiez un exemple d'événement SES dans le EventBridge Sandbox

Vous pouvez sélectionner des exemples d'événements pour les événements SES, afin de les utiliser pour tester les modèles d'événement que vous créez.

Pour spécifier un exemple d'événement SES dans le EventBridge Sandbox

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Dans le volet de navigation, choisissez Ressources pour développeurs, puis sélectionnez Environnement de test (sandbox), et sur la page Environnement de test (sandbox), choisissez l'onglet Modèle d'événement.
3. Dans Source de l'événement, choisissez AWS des événements ou des événements EventBridge partenaires.
4. Dans la section Exemple d'événement, pour Exemple de type d'événement, sélectionnez Événements AWS .
5. Pour les exemples d'événement, faites défiler la page jusqu'à SES, puis sélectionnez l'événement SES souhaité.

   EventBridge affiche un exemple d'événement, ainsi que toutes ses données détaillées, pour le type d'événement.

   Vous pouvez ensuite utiliser cet événement pour tester le modèle d'événement que vous créez dans la section Modèle d'événement, ou l'utiliser comme base pour créer vos propres exemples d'événements pour les tests de modèles décrits dans la section suivante.

Création et test de modèles d'événement pour les événements SES

Une fois que vous avez sélectionné un exemple d'événement, comme expliqué dans la section précédente, vous pouvez créer un modèle d'événement et utiliser l'exemple d'événement pour vous assurer qu'il correspond aux événements souhaités.

Pour créer et tester un modèle d'événement correspondant aux événements SES dans le EventBridge Sandbox

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Dans le volet de navigation, choisissez Ressources pour développeurs, puis sélectionnez Environnement de test (sandbox), et sur la page Environnement de test (sandbox), choisissez l'onglet Modèle d'événement.
3. Dans Source de l'événement, choisissez AWS des événements ou des événements EventBridge partenaires, puis sélectionnez l'exemple d'événement que vous souhaitez tester, comme expliqué dans la section précédente.
4. Faites défiler l'écran jusqu'à Méthode de création, puis choisissez Utiliser le formulaire de modèle.
5. Dans la section Modèle d'événement, pour Source d'événement, choisissez Services AWS .
6. Dans AWS Service, sélectionnez SES.
7. Pour Type d'événement, sélectionnez le type d'événement SES à associer.

   EventBridge affiche le modèle d'événement minimal, composé de `source` et de `detail-type` champs, qui correspond à l'événement SES sélectionné.

   Dans les deux exemples, le premier schéma d'événements correspond à tous les `Advisor Recommendation Status Resolved` événements, et dans le second, à tous les `Email Bounced` événements :

   ```
   {
     "source": ["aws.ses"],
     "detail-type": ["Advisor Recommendation Status Resolved"]
   }
   ```

   ```
   {
     "source": ["aws.ses"],
     "detail-type": ["Email Bounced"]
   }
   ```

8. Pour modifier le modèle d'événement, sélectionnez Modifier le modèle et apportez vos modifications dans l'éditeur JSON.

   Vous pouvez également faire correspondre les valeurs d'un ou de plusieurs champs de données détaillés. Cela inclut la spécification de plusieurs valeurs possibles pour une valeur de champ.

Dans l'exemple suivant, le champ détaillé a été ajouté au modèle d'événement minimal généré avec la valeur du `data` champ spécifiée `DKIM record was not found` afin de trouver tous les événements du conseiller Virtual Deliverability Manager ayant la même valeur de détail :

```
{
  "source": ["aws.ses"],
  "detail-type": ["Advisor Recommendation Status Resolved"],
  "detail": {
    "data": ["DKIM record was not found."]
  }
}
```

Dans cet exemple, des sous-champs détaillés ont été ajoutés pour signaler les événements générés par tous les e-mails envoyés par noreply@example.com le 05/08/2021 qui ont été renvoyés. (La correspondance des préfixes est utilisée ici dans le cadre du filtrage du contenu.) :

```
{
  "source": ["aws.ses"],
  "detail-type": ["Email Bounced"],
  "detail": {
    "mail": {
      "timestamp": [{
        "prefix": "2024-08-05"
      }],
      "source": ["noreply@example.com"]
    }
  }
}
```

Il est important que vous lisiez les modèles d'événements dans le guide de EventBridge l'utilisateur, qui explique que la valeur du modèle d'événement que vous entrez dans l'éditeur JSON doit être entourée de crochets `[...]` car elle est considérée comme un tableau. Ces informations, ainsi que d'autres informations sur la manière de créer des modèles d'événements avancés, sont également fournies.

9. Pour vérifier si votre modèle d'événement correspond à l'exemple d'événement que vous avez spécifié dans le volet Exemple d'événement ci-dessus, sélectionnez Tester le modèle. S'il correspond, une bannière verte en bas de l'éditeur JSON affichera : « Exemple d'événement correspondant au modèle d'événement ».

10. Pour résoudre les erreurs après avoir sélectionné le modèle de test :

    - S'il existe des erreurs liées au JSON, le message en indiquera la raison, par exemple : « Le modèle d'événement n'est pas valide. Raison : « data » doit être un objet ou un tableau à la ligne : 5, à la colonne : 14". Pour remédier à ce problème, placez la valeur de la ligne 5 entre crochets`[...]`.
    - En cas de divergence entre les valeurs de l'événement Sample et celles de votre modèle d'événement, le message sera le suivant : « L'événement de l'échantillon ne correspond pas au modèle d'événement ». Cela signifie qu'une ou plusieurs valeurs que vous souhaitez tester sont différentes des valeurs d'exemple générées par le générateur d'événements Sample. Pour y remédier, passez aux étapes restantes.

11. Pour modifier les valeurs d'échantillon dans l'événement Sample afin de tester avec succès votre modèle d'événement, dans le volet Exemple d'événement, sélectionnez Copier sous l'éditeur JSON.
12. Sélectionnez le bouton radio à côté de Enter my own pour le type d'événement Sample au-dessus de l'éditeur.
13. Collez l'exemple d'événement dans l'éditeur JSON, et pour tout champ que vous utilisez dans votre modèle d'événement, remplacez la valeur de ce même champ pour qu'elle corresponde à la valeur que vous avez spécifiée dans votre modèle d'événement.
14. Revenez au volet Modèle d'événement et sélectionnez à nouveau Modèle de test. Si toutes les valeurs ont été saisies correctement et correspondent, une bannière verte en bas de l'éditeur JSON s'affichera, intitulée « Exemple d'événement correspondant au modèle d'événement ».

EventBridge Ressources supplémentaires

Consultez les rubriques suivantes du guide de l' EventBridge utilisateur Amazon pour plus d'informations sur le traitement et la gestion des événements. EventBridge

- Pour obtenir des informations détaillées sur le fonctionnement des bus d'événements, consultez Amazon EventBridge Event Bus.
- Pour plus d'informations sur la structure des événements, consultez Événements (français non garanti)
- Pour plus d'informations sur la création de modèles d'événements EventBridge à utiliser lors de la mise en correspondance d'événements par rapport à des règles, voir Modèles d'événements

- Pour plus d'informations sur la création de règles pour spécifier quels événements EventBridge sont traités, voir Règles
- Pour plus d'informations sur la manière de spécifier les services ou autres destinations EventBridge auxquels les événements correspondants sont envoyés, voir Cibles

Exemples de code pour Amazon SES utilisant des kits SDK AWS

Les exemples de code suivants expliquent comment utiliser Amazon SES avec un kit SDK AWS.

Pour obtenir la liste complète des guides de développement AWS SDK et des exemples de code, consultez Utilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit de développement logiciel (SDK).

Exemples de code

Exemples de code pour Amazon SES à l'aide de AWS kits SDK

Les exemples de code suivants montrent comment utiliser Amazon SES avec un kit de développement AWS logiciel (SDK).

Les actions sont des extraits de code de programmes plus larges et doivent être exécutées dans leur contexte. Alors que les actions vous indiquent comment appeler des fonctions de service individuelles, vous pouvez les voir en contexte dans leurs scénarios associés et dans des exemples interservices.

Les Scénarios sont des exemples de code qui vous montrent comment accomplir une tâche spécifique en appelant plusieurs fonctions au sein d'un même service.

Les Exemples de services croisés sont des exemples d'applications fonctionnant sur plusieurs Services AWS.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit de développement logiciel (SDK).

Exemples de code

- Utilisation DeleteReceiptRule avec un AWS SDK ou une CLI
- Utilisation DeleteReceiptRuleSet avec un AWS SDK ou une CLI
- Utilisation DeleteTemplate avec un AWS SDK ou une CLI
- Utilisation DescribeReceiptRuleSet avec un AWS SDK ou une CLI
- Utilisation GetIdentityVerificationAttributes avec un AWS SDK ou une CLI
- Utilisation GetSendQuota avec un AWS SDK ou une CLI
- Utilisation GetSendStatistics avec un AWS SDK ou une CLI
- Utilisation GetTemplate avec un AWS SDK ou une CLI
- Utilisation ListIdentities avec un AWS SDK ou une CLI
- Utilisation ListReceiptFilters avec un AWS SDK ou une CLI
- Utilisation ListTemplates avec un AWS SDK ou une CLI
- Utilisation SendBulkTemplatedEmail avec un AWS SDK ou une CLI
- Utilisation SendEmail avec un AWS SDK ou une CLI
- Utilisation SendRawEmail avec un AWS SDK ou une CLI
- Utilisation SendTemplatedEmail avec un AWS SDK ou une CLI
- Utilisation UpdateTemplate avec un AWS SDK ou une CLI
- Utilisation VerifyDomainIdentity avec un AWS SDK ou une CLI
- Utilisation VerifyEmailIdentity avec un AWS SDK ou une CLI

- Scénarios pour Amazon SES utilisant des AWS kits de développement logiciel
  - Copiez les adresses e-mail et les identités de domaine Amazon SES d'une AWS région à l'autre à l'aide d'un AWS SDK
  - Générer des informations d'identification pour vous connecter à un point de terminaison d'un SMTP Amazon SES
  - Vérifiez une identité e-mail et envoyez des messages avec Amazon SES à l'aide d'un AWS SDK
- Exemples multiservices pour Amazon SES utilisant AWS des kits de développement logiciel
  - Créer une application de streaming Amazon Transcribe
  - Créer une application web pour suivre les données DynamoDB
  - Créer un outil de suivi des éléments Amazon Redshift.
  - Créer un outil de suivi des éléments de travail sans serveur Aurora
  - Détectez le PPE dans les images avec Amazon Rekognition à l'aide d'un SDK AWS
  - Détectez des objets dans des images avec Amazon Rekognition à l'aide d'un SDK AWS

- Détectez les personnes et les objets dans une vidéo avec Amazon Rekognition à l'aide d'un SDK AWS
- Utiliser les fonctions Step Functions pour invoquer des fonctions Lambda

Actions pour Amazon SES à l'aide de AWS kits SDK

Les exemples de code suivants montrent comment effectuer des actions Amazon SES individuelles avec des AWS SDK. Ces extraits appellent l'API Amazon SES et sont des extraits de code de programmes plus volumineux qui doivent être exécutés en contexte. Chaque exemple inclut un lien vers GitHub, où vous pouvez trouver des instructions pour configurer et exécuter le code.

Les exemples suivants incluent uniquement les actions les plus couramment utilisées. Pour une description complète, veuillez consulter le document Référence de l'API Amazon Simple Email Service (Amazon SES).

Exemples

- Utilisation CreateReceiptFilter avec un AWS SDK ou une CLI
- Utilisation CreateReceiptRule avec un AWS SDK ou une CLI
- Utilisation CreateReceiptRuleSet avec un AWS SDK ou une CLI
- Utilisation CreateTemplate avec un AWS SDK ou une CLI
- Utilisation DeleteIdentity avec un AWS SDK ou une CLI
- Utilisation DeleteReceiptFilter avec un AWS SDK ou une CLI
- Utilisation DeleteReceiptRule avec un AWS SDK ou une CLI
- Utilisation DeleteReceiptRuleSet avec un AWS SDK ou une CLI
- Utilisation DeleteTemplate avec un AWS SDK ou une CLI
- Utilisation DescribeReceiptRuleSet avec un AWS SDK ou une CLI
- Utilisation GetIdentityVerificationAttributes avec un AWS SDK ou une CLI
- Utilisation GetSendQuota avec un AWS SDK ou une CLI
- Utilisation GetSendStatistics avec un AWS SDK ou une CLI
- Utilisation GetTemplate avec un AWS SDK ou une CLI
- Utilisation ListIdentities avec un AWS SDK ou une CLI
- Utilisation ListReceiptFilters avec un AWS SDK ou une CLI
- Utilisation ListTemplates avec un AWS SDK ou une CLI

- Utilisation SendBulkTemplatedEmail avec un AWS SDK ou une CLI
- Utilisation SendEmail avec un AWS SDK ou une CLI
- Utilisation SendRawEmail avec un AWS SDK ou une CLI
- Utilisation SendTemplatedEmail avec un AWS SDK ou une CLI
- Utilisation UpdateTemplate avec un AWS SDK ou une CLI
- Utilisation VerifyDomainIdentity avec un AWS SDK ou une CLI
- Utilisation VerifyEmailIdentity avec un AWS SDK ou une CLI

Utilisation **`CreateReceiptFilter`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`CreateReceiptFilter`.

C++

Kit de développement logiciel (SDK) for C++

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
//! Create an Amazon Simple Email Service (Amazon SES) receipt filter..
/*!
  \param receiptFilterName: The name for the receipt filter.
  \param cidr: IP address or IP address range in Classless Inter-Domain Routing
 (CIDR) notation.
  \param policy: Block or allow enum of type ReceiptFilterPolicy.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::createReceiptFilter(const Aws::String &receiptFilterName,
                                      const Aws::String &cidr,
                                      Aws::SES::Model::ReceiptFilterPolicy
 policy,
                                      const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);
    Aws::SES::Model::CreateReceiptFilterRequest createReceiptFilterRequest;
```

```
    Aws::SES::Model::ReceiptFilter receiptFilter;
    Aws::SES::Model::ReceiptIpFilter receiptIpFilter;
    receiptIpFilter.SetCidr(cidr);
    receiptIpFilter.SetPolicy(policy);
    receiptFilter.SetName(receiptFilterName);
    receiptFilter.SetIpFilter(receiptIpFilter);
    createReceiptFilterRequest.SetFilter(receiptFilter);
    Aws::SES::Model::CreateReceiptFilterOutcome createReceiptFilterOutcome =
 sesClient.CreateReceiptFilter(
            createReceiptFilterRequest);
    if (createReceiptFilterOutcome.IsSuccess()) {
        std::cout << "Successfully created receipt filter." << std::endl;
    }
    else {
        std::cerr << "Error creating receipt filter: " <<
                  createReceiptFilterOutcome.GetError().GetMessage() <<
 std::endl;
    }

    return createReceiptFilterOutcome.IsSuccess();
}
```

- Pour plus de détails sur l'API, reportez-vous CreateReceiptFilterà la section Référence des AWS SDK for C++ API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import {
  CreateReceiptFilterCommand,
  ReceiptFilterPolicy,
} from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";
```

```
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";

const createCreateReceiptFilterCommand = ({ policy, ipOrRange, name }) => {
  return new CreateReceiptFilterCommand({
    Filter: {
      IpFilter: {
        Cidr: ipOrRange, // string, either a single IP address (10.0.0.1) or an
 IP address range in CIDR notation (10.0.0.1/24)).
        Policy: policy, // enum ReceiptFilterPolicy, email traffic from the
 filtered addressesOptions.
      },
      /*
        The name of the IP address filter. Only ASCII letters, numbers,
 underscores, or dashes.
        Must be less than 64 characters and start and end with a letter or
 number.
       */
      Name: name,
    },
  });
};

const FILTER_NAME = getUniqueName("ReceiptFilter");

const run = async () => {
  const createReceiptFilterCommand = createCreateReceiptFilterCommand({
    policy: ReceiptFilterPolicy.Allow,
    ipOrRange: "10.0.0.1",
    name: FILTER_NAME,
  });

  try {
    return await sesClient.send(createReceiptFilterCommand);
  } catch (caught) {
    if (caught instanceof Error && caught.name === "MessageRejected") {
      /** @type { import('@aws-sdk/client-ses').MessageRejected} */
      const messageRejectedError = caught;
      return messageRejectedError;
    }
    throw caught;
  }
};
```

- Pour plus de détails sur l'API, reportez-vous CreateReceiptFilterà la section Référence des AWS SDK for JavaScript API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SesReceiptHandler:
    """Encapsulates Amazon SES receipt handling functions."""

    def __init__(self, ses_client, s3_resource):
        """
        :param ses_client: A Boto3 Amazon SES client.
        :param s3_resource: A Boto3 Amazon S3 resource.
        """
        self.ses_client = ses_client
        self.s3_resource = s3_resource


    def create_receipt_filter(self, filter_name, ip_address_or_range, allow):
        """
        Creates a filter that allows or blocks incoming mail from an IP address
 or
        range.

        :param filter_name: The name to give the filter.
        :param ip_address_or_range: The IP address or range to block or allow.
        :param allow: When True, incoming mail is allowed from the specified IP
                      address or range; otherwise, it is blocked.
        """
        try:
            policy = "Allow" if allow else "Block"
            self.ses_client.create_receipt_filter(
```

```
                Filter={
                    "Name": filter_name,
                    "IpFilter": {"Cidr": ip_address_or_range, "Policy": policy},
                }
            )
            logger.info(
                "Created receipt filter %s to %s IP of %s.",
                filter_name,
                policy,
                ip_address_or_range,
            )
        except ClientError:
            logger.exception("Couldn't create receipt filter %s.", filter_name)
            raise
```

- Pour plus de détails sur l'API, consultez CreateReceiptFilterle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`CreateReceiptRule`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`CreateReceiptRule`.

C++

Kit de développement logiciel (SDK) for C++

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
//! Create an Amazon Simple Email Service (Amazon SES) receipt rule.
/*!
  \param receiptRuleName: The name for the receipt rule.
```

```
  \param s3BucketName: The name of the S3 bucket for incoming mail.
  \param s3ObjectKeyPrefix: The prefix for the objects in the S3 bucket.
  \param ruleSetName: The name of the rule set where the receipt rule is added.
  \param recipients: Aws::Vector of recipients.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::createReceiptRule(const Aws::String &receiptRuleName,
                                    const Aws::String &s3BucketName,
                                    const Aws::String &s3ObjectKeyPrefix,
                                    const Aws::String &ruleSetName,
                                    const Aws::Vector<Aws::String> &recipients,
                                    const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::CreateReceiptRuleRequest createReceiptRuleRequest;

    Aws::SES::Model::S3Action s3Action;
    s3Action.SetBucketName(s3BucketName);
    s3Action.SetObjectKeyPrefix(s3ObjectKeyPrefix);

    Aws::SES::Model::ReceiptAction receiptAction;
    receiptAction.SetS3Action(s3Action);

    Aws::SES::Model::ReceiptRule receiptRule;
    receiptRule.SetName(receiptRuleName);
    receiptRule.WithRecipients(recipients);

    Aws::Vector<Aws::SES::Model::ReceiptAction> receiptActionList;
    receiptActionList.emplace_back(receiptAction);
    receiptRule.SetActions(receiptActionList);

    createReceiptRuleRequest.SetRuleSetName(ruleSetName);
    createReceiptRuleRequest.SetRule(receiptRule);

    auto outcome = sesClient.CreateReceiptRule(createReceiptRuleRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully created receipt rule." << std::endl;
    }
    else {
        std::cerr << "Error creating receipt rule. " <<
 outcome.GetError().GetMessage()
```

```
                    << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Pour plus de détails sur l'API, reportez-vous CreateReceiptRuleà la section Référence des AWS SDK for C++ API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { CreateReceiptRuleCommand, TlsPolicy } from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";

const RULE_SET_NAME = getUniqueName("RuleSetName");
const RULE_NAME = getUniqueName("RuleName");
const S3_BUCKET_NAME = getUniqueName("S3BucketName");

const createS3ReceiptRuleCommand = ({
  bucketName,
  emailAddresses,
  name,
  ruleSet,
}) => {
  return new CreateReceiptRuleCommand({
    Rule: {
      Actions: [
        {
          S3Action: {
            BucketName: bucketName,
```

```
            ObjectKeyPrefix: "email",
          },
        },
      ],
      Recipients: emailAddresses,
      Enabled: true,
      Name: name,
      ScanEnabled: false,
      TlsPolicy: TlsPolicy.Optional,
    },
    RuleSetName: ruleSet, // Required
  });
};

const run = async () => {
  const s3ReceiptRuleCommand = createS3ReceiptRuleCommand({
    bucketName: S3_BUCKET_NAME,
    emailAddresses: ["email@example.com"],
    name: RULE_NAME,
    ruleSet: RULE_SET_NAME,
  });

  try {
    return await sesClient.send(s3ReceiptRuleCommand);
  } catch (err) {
    console.log("Failed to create S3 receipt rule.", err);
    throw err;
  }
};
```

- Pour plus de détails sur l'API, reportez-vous CreateReceiptRuleà la section Référence des AWS SDK for JavaScript API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Créez un compartiment Amazon S3 où Amazon SES peut placer des copies d'e-mails entrants et créez une règle qui copie les e-mails entrants dans le compartiment pour une liste spécifique de destinataires.

```
class SesReceiptHandler:
    """Encapsulates Amazon SES receipt handling functions."""

    def __init__(self, ses_client, s3_resource):
        """
        :param ses_client: A Boto3 Amazon SES client.
        :param s3_resource: A Boto3 Amazon S3 resource.
        """
        self.ses_client = ses_client
        self.s3_resource = s3_resource


    def create_bucket_for_copy(self, bucket_name):
        """
        Creates a bucket that can receive copies of emails from Amazon SES. This
        includes adding a policy to the bucket that grants Amazon SES permission
        to put objects in the bucket.

        :param bucket_name: The name of the bucket to create.
        :return: The newly created bucket.
        """
        allow_ses_put_policy = {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "AllowSESPut",
                    "Effect": "Allow",
                    "Principal": {"Service": "ses.amazonaws.com"},
```

```
                    "Action": "s3:PutObject",
                    "Resource": f"arn:aws:s3:::{bucket_name}/*",
                }
            ],
        }
        bucket = None
        try:
            bucket = self.s3_resource.create_bucket(
                Bucket=bucket_name,
                CreateBucketConfiguration={
                    "LocationConstraint":
self.s3_resource.meta.client.meta.region_name
                },
            )
            bucket.wait_until_exists()
            bucket.Policy().put(Policy=json.dumps(allow_ses_put_policy))
            logger.info("Created bucket %s to receive copies of emails.",
bucket_name)
        except ClientError:
            logger.exception("Couldn't create bucket to receive copies of
emails.")
            if bucket is not None:
                bucket.delete()
            raise
        else:
            return bucket


    def create_s3_copy_rule(
        self, rule_set_name, rule_name, recipients, bucket_name, prefix
    ):
        """
        Creates a rule so that all emails received by the specified recipients
are
        copied to an Amazon S3 bucket.

        :param rule_set_name: The name of a previously created rule set to
contain
                              this rule.
        :param rule_name: The name to give the rule.
        :param recipients: When an email is received by one of these recipients,
it
                           is copied to the Amazon S3 bucket.
        :param bucket_name: The name of the bucket to receive email copies. This
```

```
                            bucket must allow Amazon SES to put objects into it.
        :param prefix: An object key prefix to give the emails copied to the
bucket.
        """
        try:
            self.ses_client.create_receipt_rule(
                RuleSetName=rule_set_name,
                Rule={
                    "Name": rule_name,
                    "Enabled": True,
                    "Recipients": recipients,
                    "Actions": [
                        {
                            "S3Action": {
                                "BucketName": bucket_name,
                                "ObjectKeyPrefix": prefix,
                            }
                        }
                    ],
                },
            )
            logger.info(
                "Created rule %s to copy mail received by %s to bucket %s.",
                rule_name,
                recipients,
                bucket_name,
            )
        except ClientError:
            logger.exception("Couldn't create rule %s.", rule_name)
            raise
```

- Pour plus de détails sur l'API, consultez CreateReceiptRulele AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`CreateReceiptRuleSet`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`CreateReceiptRuleSet`.

C++

Kit de développement logiciel (SDK) for C++

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
//! Create an Amazon Simple Email Service (Amazon SES) receipt rule set.
/*!
  \param ruleSetName: The name of the rule set.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::createReceiptRuleSet(const Aws::String &ruleSetName,
                                       const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::CreateReceiptRuleSetRequest createReceiptRuleSetRequest;

    createReceiptRuleSetRequest.SetRuleSetName(ruleSetName);

    Aws::SES::Model::CreateReceiptRuleSetOutcome outcome =
 sesClient.CreateReceiptRuleSet(
            createReceiptRuleSetRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully created receipt rule set." << std::endl;
    }
    else {
        std::cerr << "Error creating receipt rule set. "
                  << outcome.GetError().GetMessage()
                  << std::endl;
    }
```

```
    return outcome.IsSuccess();
}
```

- Pour plus de détails sur l'API, voir CreateReceiptRuleSetla section Référence des AWS SDK for C++ API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { CreateReceiptRuleSetCommand } from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";

const RULE_SET_NAME = getUniqueName("RuleSetName");

const createCreateReceiptRuleSetCommand = (ruleSetName) => {
  return new CreateReceiptRuleSetCommand({ RuleSetName: ruleSetName });
};

const run = async () => {
  const createReceiptRuleSetCommand =
    createCreateReceiptRuleSetCommand(RULE_SET_NAME);

  try {
    return await sesClient.send(createReceiptRuleSetCommand);
  } catch (err) {
    console.log("Failed to create receipt rule set", err);
    return err;
  }
};
```

- Pour plus de détails sur l'API, voir CreateReceiptRuleSetla section Référence des AWS SDK for JavaScript API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SesReceiptHandler:
    """Encapsulates Amazon SES receipt handling functions."""

    def __init__(self, ses_client, s3_resource):
        """
        :param ses_client: A Boto3 Amazon SES client.
        :param s3_resource: A Boto3 Amazon S3 resource.
        """
        self.ses_client = ses_client
        self.s3_resource = s3_resource


    def create_receipt_rule_set(self, rule_set_name):
        """
        Creates an empty rule set. Rule sets contain individual rules and can be
        used to organize rules.

        :param rule_set_name: The name to give the rule set.
        """
        try:
            self.ses_client.create_receipt_rule_set(RuleSetName=rule_set_name)
            logger.info("Created receipt rule set %s.", rule_set_name)
        except ClientError:
            logger.exception("Couldn't create receipt rule set %s.",
 rule_set_name)
            raise
```

- Pour plus de détails sur l'API, consultez CreateReceiptRuleSetle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`CreateTemplate`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`CreateTemplate`.

Les exemples d’actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l’exemple de code suivant :

- Vérifier une identité d'e-mail et envoyer des messages

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   /// <summary>
   /// Create an email template.
   /// </summary>
   /// <param name="name">Name of the template.</param>
   /// <param name="subject">Email subject.</param>
   /// <param name="text">Email body text.</param>
   /// <param name="html">Email HTML body text.</param>
   /// <returns>True if successful.</returns>
   public async Task<bool> CreateEmailTemplateAsync(string name, string subject,
string text,
       string html)
   {
```

```
        var success = false;
        try
        {
            var response = await _amazonSimpleEmailService.CreateTemplateAsync(
                new CreateTemplateRequest
                {
                    Template = new Template
                    {
                        TemplateName = name,
                        SubjectPart = subject,
                        TextPart = text,
                        HtmlPart = html
                    }
                });
            success = response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (Exception ex)
        {
            Console.WriteLine("CreateEmailTemplateAsync failed with exception: "
+ ex.Message);
        }

        return success;
    }
```

- Pour plus de détails sur l'API, voir CreateTemplatela section Référence des AWS SDK for .NET API.

C++

SDK pour C++

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
//! Create an Amazon Simple Email Service (Amazon SES) template.
```

```
/*!
  \param templateName: The name of the template.
  \param htmlPart: The HTML body of the email.
  \param subjectPart: The subject line of the email.
  \param textPart: The plain text version of the email.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::createTemplate(const Aws::String &templateName,
                                 const Aws::String &htmlPart,
                                 const Aws::String &subjectPart,
                                 const Aws::String &textPart,
                                 const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::CreateTemplateRequest createTemplateRequest;
    Aws::SES::Model::Template aTemplate;

    aTemplate.SetTemplateName(templateName);
    aTemplate.SetHtmlPart(htmlPart);
    aTemplate.SetSubjectPart(subjectPart);
    aTemplate.SetTextPart(textPart);

    createTemplateRequest.SetTemplate(aTemplate);

    Aws::SES::Model::CreateTemplateOutcome outcome = sesClient.CreateTemplate(
            createTemplateRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully created template." << templateName << "."
                  << std::endl;
    }
    else {
        std::cerr << "Error creating template. " <<
 outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Pour plus de détails sur l'API, voir CreateTemplatela section Référence des AWS SDK for C ++ API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { CreateTemplateCommand } from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";

const TEMPLATE_NAME = getUniqueName("TestTemplateName");

const createCreateTemplateCommand = () => {
  return new CreateTemplateCommand({
    /**
     * The template feature in Amazon SES is based on the Handlebars template
 system.
     */
    Template: {
      /**
       * The name of an existing template in Amazon SES.
       */
      TemplateName: TEMPLATE_NAME,
      HtmlPart: `
        <h1>Hello, {{contact.firstName}}!</h1>
        <p>
        Did you know Amazon has a mascot named Peccy?
        </p>
      `,
      SubjectPart: "Amazon Tip",
    },
  });
};
```

```
const run = async () => {
  const createTemplateCommand = createCreateTemplateCommand();

  try {
    return await sesClient.send(createTemplateCommand);
  } catch (err) {
    console.log("Failed to create template.", err);
    return err;
  }
};
```

- Pour plus de détails sur l'API, voir CreateTemplatela section Référence des AWS SDK for JavaScript API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SesTemplate:
    """Encapsulates Amazon SES template functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client
        self.template = None
        self.template_tags = set()

    def _extract_tags(self, subject, text, html):
        """
        Extracts tags from a template as a set of unique values.
```

```
        :param subject: The subject of the email.
        :param text: The text version of the email.
        :param html: The html version of the email.
        """
        self.template_tags = set(re.findall(TEMPLATE_REGEX, subject + text +
html))
        logger.info("Extracted template tags: %s", self.template_tags)


    def create_template(self, name, subject, text, html):
        """
        Creates an email template.

        :param name: The name of the template.
        :param subject: The subject of the email.
        :param text: The plain text version of the email.
        :param html: The HTML version of the email.
        """
        try:
            template = {
                "TemplateName": name,
                "SubjectPart": subject,
                "TextPart": text,
                "HtmlPart": html,
            }
            self.ses_client.create_template(Template=template)
            logger.info("Created template %s.", name)
            self.template = template
            self._extract_tags(subject, text, html)
        except ClientError:
            logger.exception("Couldn't create template %s.", name)
            raise
```

- Pour plus de détails sur l'API, consultez CreateTemplatele AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DeleteIdentity`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`DeleteIdentity`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Vérifier une identité d'e-mail et envoyer des messages

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
/// <summary>
/// Delete an email identity.
/// </summary>
/// <param name="identityEmail">The identity email to delete.</param>
/// <returns>True if successful.</returns>
public async Task<bool> DeleteIdentityAsync(string identityEmail)
{
    var success = false;
    try
    {
        var response = await _amazonSimpleEmailService.DeleteIdentityAsync(
            new DeleteIdentityRequest
            {
                Identity = identityEmail
            });
        success = response.HttpStatusCode == HttpStatusCode.OK;
    }
    catch (Exception ex)
    {
```

```
            Console.WriteLine("DeleteIdentityAsync failed with exception: " +
 ex.Message);
        }

        return success;
    }
```

- Pour plus de détails sur l'API, voir DeleteIdentityla section Référence des AWS SDK for .NET API.

C++

SDK pour C++

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
//! Delete the specified identity (an email address or a domain).
/*!
  \param identity: The identity to delete.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::deleteIdentity(const Aws::String &identity,
                                 const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::DeleteIdentityRequest deleteIdentityRequest;

    deleteIdentityRequest.SetIdentity(identity);

    Aws::SES::Model::DeleteIdentityOutcome outcome = sesClient.DeleteIdentity(
            deleteIdentityRequest);

    if (outcome.IsSuccess()) {
```

```
        std::cout << "Successfully deleted identity." << std::endl;
    }
    else {
        std::cerr << "Error deleting identity. " <<
 outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Pour plus de détails sur l'API, voir DeleteIdentityla section Référence des AWS SDK for C++ API.

CLI

AWS CLI

Pour supprimer une identité

L'exemple suivant utilise la commande `delete-identity` pour supprimer une identité de la liste des identités vérifiées auprès d'Amazon SES :

```
aws ses delete-identity --identity user@example.com
```

Pour plus d'informations sur les identités vérifiées, consultez Vérification des adresses e-mail et des domaines dans Amazon SES dans le Guide du développeur Amazon Simple Email Service.

- Pour plus de détails sur l'API, voir DeleteIdentityla section Référence des AWS CLI commandes.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { DeleteIdentityCommand } from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";

const IDENTITY_EMAIL = "fake@example.com";

const createDeleteIdentityCommand = (identityName) => {
  return new DeleteIdentityCommand({
    Identity: identityName,
  });
};

const run = async () => {
  const deleteIdentityCommand = createDeleteIdentityCommand(IDENTITY_EMAIL);

  try {
    return await sesClient.send(deleteIdentityCommand);
  } catch (err) {
    console.log("Failed to delete identity.", err);
    return err;
  }
};
```

- Pour plus de détails sur l'API, voir DeleteIdentityla section Référence des AWS SDK for JavaScript API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SesIdentity:
    """Encapsulates Amazon SES identity functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client


    def delete_identity(self, identity):
        """
        Deletes an identity.

        :param identity: The identity to remove.
        """
        try:
            self.ses_client.delete_identity(Identity=identity)
            logger.info("Deleted identity %s.", identity)
        except ClientError:
            logger.exception("Couldn't delete identity %s.", identity)
            raise
```

- Pour plus de détails sur l'API, consultez DeleteIdentityle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DeleteReceiptFilter`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`DeleteReceiptFilter`.

C++

Kit de développement logiciel (SDK) for C++

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
//! Delete an Amazon Simple Email Service (Amazon SES) receipt filter.
/*!
  \param receiptFilterName: The name for the receipt filter.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::deleteReceiptFilter(const Aws::String &receiptFilterName,
                                      const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::DeleteReceiptFilterRequest deleteReceiptFilterRequest;

    deleteReceiptFilterRequest.SetFilterName(receiptFilterName);

    Aws::SES::Model::DeleteReceiptFilterOutcome outcome =
 sesClient.DeleteReceiptFilter(
            deleteReceiptFilterRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully deleted receipt filter." << std::endl;
    }
    else {
        std::cerr << "Error deleting receipt filter. "
                  << outcome.GetError().GetMessage()
                  << std::endl;
    }
```

```
    return outcome.IsSuccess();
}
```

- Pour plus de détails sur l'API, voir DeleteReceiptFilterla section Référence des AWS SDK for C++ API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { DeleteReceiptFilterCommand } from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";

const RECEIPT_FILTER_NAME = getUniqueName("ReceiptFilterName");

const createDeleteReceiptFilterCommand = (filterName) => {
  return new DeleteReceiptFilterCommand({ FilterName: filterName });
};

const run = async () => {
  const deleteReceiptFilterCommand =
    createDeleteReceiptFilterCommand(RECEIPT_FILTER_NAME);

  try {
    return await sesClient.send(deleteReceiptFilterCommand);
  } catch (err) {
    console.log("Error deleting receipt filter.", err);
    return err;
  }
};
```

- Pour plus de détails sur l'API, voir DeleteReceiptFilterla section Référence des AWS SDK for JavaScript API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SesReceiptHandler:
    """Encapsulates Amazon SES receipt handling functions."""

    def __init__(self, ses_client, s3_resource):
        """
        :param ses_client: A Boto3 Amazon SES client.
        :param s3_resource: A Boto3 Amazon S3 resource.
        """
        self.ses_client = ses_client
        self.s3_resource = s3_resource


    def delete_receipt_filter(self, filter_name):
        """
        Deletes a receipt filter.

        :param filter_name: The name of the filter to delete.
        """
        try:
            self.ses_client.delete_receipt_filter(FilterName=filter_name)
            logger.info("Deleted receipt filter %s.", filter_name)
        except ClientError:
            logger.exception("Couldn't delete receipt filter %s.", filter_name)
            raise
```

- Pour plus de détails sur l'API, consultez DeleteReceiptFilterle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DeleteReceiptRule`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`DeleteReceiptRule`.

C++

Kit de développement logiciel (SDK) for C++

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
//! Delete an Amazon Simple Email Service (Amazon SES) receipt rule.
/*!
  \param receiptRuleName: The name for the receipt rule.
  \param receiptRuleSetName: The name for the receipt rule set.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::deleteReceiptRule(const Aws::String &receiptRuleName,
                                    const Aws::String &receiptRuleSetName,
                                    const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::DeleteReceiptRuleRequest deleteReceiptRuleRequest;

    deleteReceiptRuleRequest.SetRuleName(receiptRuleName);
    deleteReceiptRuleRequest.SetRuleSetName(receiptRuleSetName);

    Aws::SES::Model::DeleteReceiptRuleOutcome outcome =
 sesClient.DeleteReceiptRule(
```

```
            deleteReceiptRuleRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully deleted receipt rule." << std::endl;
    }
    else {
        std::cout << "Error deleting receipt rule. " <<
 outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Pour plus de détails sur l'API, voir DeleteReceiptRulela section Référence des AWS SDK for C++ API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { DeleteReceiptRuleCommand } from "@aws-sdk/client-ses";
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";
import { sesClient } from "./libs/sesClient.js";

const RULE_NAME = getUniqueName("RuleName");
const RULE_SET_NAME = getUniqueName("RuleSetName");

const createDeleteReceiptRuleCommand = () => {
  return new DeleteReceiptRuleCommand({
    RuleName: RULE_NAME,
    RuleSetName: RULE_SET_NAME,
  });
```

```
};

const run = async () => {
  const deleteReceiptRuleCommand = createDeleteReceiptRuleCommand();
  try {
    return await sesClient.send(deleteReceiptRuleCommand);
  } catch (err) {
    console.log("Failed to delete receipt rule.", err);
    return err;
  }
};
```

- Pour plus de détails sur l'API, voir DeleteReceiptRulela section Référence des AWS SDK for JavaScript API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SesReceiptHandler:
    """Encapsulates Amazon SES receipt handling functions."""

    def __init__(self, ses_client, s3_resource):
        """
        :param ses_client: A Boto3 Amazon SES client.
        :param s3_resource: A Boto3 Amazon S3 resource.
        """
        self.ses_client = ses_client
        self.s3_resource = s3_resource


    def delete_receipt_rule(self, rule_set_name, rule_name):
        """
        Deletes a rule.
```

```
        :param rule_set_name: The rule set that contains the rule to delete.
        :param rule_name: The rule to delete.
        """
        try:
            self.ses_client.delete_receipt_rule(
                RuleSetName=rule_set_name, RuleName=rule_name
            )
            logger.info("Removed rule %s from rule set %s.", rule_name,
rule_set_name)
        except ClientError:
            logger.exception(
                "Couldn't remove rule %s from rule set %s.", rule_name,
rule_set_name
            )
            raise
```

- Pour plus de détails sur l'API, consultez DeleteReceiptRulele AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DeleteReceiptRuleSet`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`DeleteReceiptRuleSet`.

C++

Kit de développement logiciel (SDK) for C++

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
//! Delete an Amazon Simple Email Service (Amazon SES) receipt rule set.
```

```
/*!
  \param receiptRuleSetName: The name for the receipt rule set.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::deleteReceiptRuleSet(const Aws::String &receiptRuleSetName,
                                       const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::DeleteReceiptRuleSetRequest deleteReceiptRuleSetRequest;

    deleteReceiptRuleSetRequest.SetRuleSetName(receiptRuleSetName);

    Aws::SES::Model::DeleteReceiptRuleSetOutcome outcome =
 sesClient.DeleteReceiptRuleSet(
            deleteReceiptRuleSetRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully deleted receipt rule set." << std::endl;
    }

    else {
        std::cerr << "Error deleting receipt rule set. "
                  << outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Pour plus de détails sur l'API, voir DeleteReceiptRuleSetla section Référence des AWS SDK for C++ API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { DeleteReceiptRuleSetCommand } from "@aws-sdk/client-ses";
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";
import { sesClient } from "./libs/sesClient.js";

const RULE_SET_NAME = getUniqueName("RuleSetName");

const createDeleteReceiptRuleSetCommand = () => {
  return new DeleteReceiptRuleSetCommand({ RuleSetName: RULE_SET_NAME });
};

const run = async () => {
  const deleteReceiptRuleSetCommand = createDeleteReceiptRuleSetCommand();

  try {
    return await sesClient.send(deleteReceiptRuleSetCommand);
  } catch (err) {
    console.log("Failed to delete receipt rule set.", err);
    return err;
  }
};
```

- Pour plus de détails sur l'API, voir DeleteReceiptRuleSetla section Référence des AWS SDK for JavaScript API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SesReceiptHandler:
    """Encapsulates Amazon SES receipt handling functions."""

    def __init__(self, ses_client, s3_resource):
        """
        :param ses_client: A Boto3 Amazon SES client.
        :param s3_resource: A Boto3 Amazon S3 resource.
        """
        self.ses_client = ses_client
        self.s3_resource = s3_resource


    def delete_receipt_rule_set(self, rule_set_name):
        """
        Deletes a rule set. When a rule set is deleted, all of the rules it
 contains
        are also deleted.

        :param rule_set_name: The name of the rule set to delete.
        """
        try:
            self.ses_client.delete_receipt_rule_set(RuleSetName=rule_set_name)
            logger.info("Deleted rule set %s.", rule_set_name)
        except ClientError:
            logger.exception("Couldn't delete rule set %s.", rule_set_name)
            raise
```

- Pour plus de détails sur l'API, consultez DeleteReceiptRuleSetle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DeleteTemplate`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`DeleteTemplate`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Vérifier une identité d'e-mail et envoyer des messages

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
/// <summary>
/// Delete an email template.
/// </summary>
/// <param name="templateName">Name of the template.</param>
/// <returns>True if successful.</returns>
public async Task<bool> DeleteEmailTemplateAsync(string templateName)
{
    var success = false;
    try
    {
        var response = await _amazonSimpleEmailService.DeleteTemplateAsync(
            new DeleteTemplateRequest
            {
                TemplateName = templateName
            });
        success = response.HttpStatusCode == HttpStatusCode.OK;
```

```
        }
        catch (Exception ex)
        {
            Console.WriteLine("DeleteEmailTemplateAsync failed with exception: "
 + ex.Message);
        }

        return success;
    }
```

- Pour plus de détails sur l'API, voir DeleteTemplatela section Référence des AWS SDK for .NET API.

C++

SDK pour C++

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
//! Delete an Amazon Simple Email Service (Amazon SES) template.
/*!
  \param templateName: The name for the template.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::deleteTemplate(const Aws::String &templateName,
                                 const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::DeleteTemplateRequest deleteTemplateRequest;

    deleteTemplateRequest.SetTemplateName(templateName);

    Aws::SES::Model::DeleteTemplateOutcome outcome = sesClient.DeleteTemplate(
```

```
            deleteTemplateRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully deleted template." << std::endl;
    }
    else {
        std::cerr << "Error deleting template. " <<
 outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Pour plus de détails sur l'API, voir DeleteTemplatela section Référence des AWS SDK for C ++ API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { DeleteTemplateCommand } from "@aws-sdk/client-ses";
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";
import { sesClient } from "./libs/sesClient.js";

const TEMPLATE_NAME = getUniqueName("TemplateName");

const createDeleteTemplateCommand = (templateName) =>
  new DeleteTemplateCommand({ TemplateName: templateName });

const run = async () => {
  const deleteTemplateCommand = createDeleteTemplateCommand(TEMPLATE_NAME);
```

```
  try {
    return await sesClient.send(deleteTemplateCommand);
  } catch (err) {
    console.log("Failed to delete template.", err);
    return err;
  }
};
```

- Pour plus de détails sur l'API, voir DeleteTemplatela section Référence des AWS SDK for JavaScript API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SesTemplate:
    """Encapsulates Amazon SES template functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client
        self.template = None
        self.template_tags = set()

    def _extract_tags(self, subject, text, html):
        """
        Extracts tags from a template as a set of unique values.

        :param subject: The subject of the email.
        :param text: The text version of the email.
        :param html: The html version of the email.
        """
```

```
        self.template_tags = set(re.findall(TEMPLATE_REGEX, subject + text +
html))
        logger.info("Extracted template tags: %s", self.template_tags)


    def delete_template(self):
        """
        Deletes an email template.
        """
        try:

self.ses_client.delete_template(TemplateName=self.template["TemplateName"])
            logger.info("Deleted template %s.", self.template["TemplateName"])
            self.template = None
            self.template_tags = None
        except ClientError:
            logger.exception(
                "Couldn't delete template %s.", self.template["TemplateName"]
            )
            raise
```

- Pour plus de détails sur l'API, consultez DeleteTemplatele AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DescribeReceiptRuleSet`** avec un AWS SDK ou une CLI

L'exemple de code suivant montre comment utiliser`DescribeReceiptRuleSet`.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SesReceiptHandler:
    """Encapsulates Amazon SES receipt handling functions."""

    def __init__(self, ses_client, s3_resource):
        """
        :param ses_client: A Boto3 Amazon SES client.
        :param s3_resource: A Boto3 Amazon S3 resource.
        """
        self.ses_client = ses_client
        self.s3_resource = s3_resource


    def describe_receipt_rule_set(self, rule_set_name):
        """
        Gets data about a rule set.

        :param rule_set_name: The name of the rule set to retrieve.
        :return: Data about the rule set.
        """
        try:
            response = self.ses_client.describe_receipt_rule_set(
                RuleSetName=rule_set_name
            )
            logger.info("Got data for rule set %s.", rule_set_name)
        except ClientError:
            logger.exception("Couldn't get data for rule set %s.", rule_set_name)
            raise
        else:
            return response
```

- Pour plus de détails sur l'API, consultez DescribeReceiptRuleSetle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`GetIdentityVerificationAttributes`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`GetIdentityVerificationAttributes`.

Les exemples d’actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l’exemple de code suivant :

- Vérifier une identité d'e-mail et envoyer des messages

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
/// <summary>
/// Get identity verification status for an email.
/// </summary>
/// <returns>The verification status of the email.</returns>
public async Task<VerificationStatus> GetIdentityStatusAsync(string email)
{
    var result = VerificationStatus.TemporaryFailure;
    try
    {
        var response =
```

```
                await
_amazonSimpleEmailService.GetIdentityVerificationAttributesAsync(
                    new GetIdentityVerificationAttributesRequest
                    {
                        Identities = new List<string> { email }
                    });

            if (response.VerificationAttributes.ContainsKey(email))
                result =
response.VerificationAttributes[email].VerificationStatus;
        }
        catch (Exception ex)
        {
            Console.WriteLine("GetIdentityStatusAsync failed with exception: " +
ex.Message);
        }

        return result;
    }
```

- Pour plus de détails sur l'API, voir GetIdentityVerificationAttributesla section Référence des AWS SDK for .NET API.

CLI

AWS CLI

Pour obtenir le statut de vérification Amazon SES pour une liste d'identités

L'exemple suivant utilise la commande `get-identity-verification-attributes` pour récupérer le statut de vérification Amazon SES pour une liste d'identités :

```
aws ses get-identity-verification-attributes --identities "user1@example.com"
 "user2@example.com"
```

Sortie :

```
{
   "VerificationAttributes": {
       "user1@example.com": {
```

```
            "VerificationStatus": "Success"
        },
        "user2@example.com": {
            "VerificationStatus": "Pending"
        }
    }
}
```

Si vous appelez cette commande avec une identité que vous n'avez jamais soumise pour vérification, cette identité n'apparaîtra pas dans la sortie.

Pour plus d'informations sur les identités vérifiées, consultez Vérification des adresses e-mail et des domaines dans Amazon SES dans le Guide du développeur Amazon Simple Email Service.

- Pour plus de détails sur l'API, voir GetIdentityVerificationAttributesla section Référence des AWS CLI commandes.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SesIdentity:
    """Encapsulates Amazon SES identity functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client


    def get_identity_status(self, identity):
        """
        Gets the status of an identity. This can be used to discover whether
```

```
        an identity has been successfully verified.

        :param identity: The identity to query.
        :return: The status of the identity.
        """
        try:
            response = self.ses_client.get_identity_verification_attributes(
                Identities=[identity]
            )
            status = response["VerificationAttributes"].get(
                identity, {"VerificationStatus": "NotFound"}
            )["VerificationStatus"]
            logger.info("Got status of %s for %s.", status, identity)
        except ClientError:
            logger.exception("Couldn't get status for %s.", identity)
            raise
        else:
            return status
```

- Pour plus de détails sur l'API, consultez GetIdentityVerificationAttributesle AWS manuel de référence de l'API SDK for Python (Boto3).

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
require "aws-sdk-ses"  # v2: require 'aws-sdk'

# Create client in us-west-2 region
# Replace us-west-2 with the AWS Region you're using for Amazon SES.
client = Aws::SES::Client.new(region: "us-west-2")
```

```
# Get up to 1000 identities
ids = client.list_identities({
  identity_type: "EmailAddress"
})

ids.identities.each do |email|
  attrs = client.get_identity_verification_attributes({
    identities: [email]
  })

  status = attrs.verification_attributes[email].verification_status

  # Display email addresses that have been verified
  if status == "Success"
    puts email
  end
end
```

- Pour plus de détails sur l'API, voir GetIdentityVerificationAttributesla section Référence des AWS SDK for Ruby API.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`GetSendQuota`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`GetSendQuota`.

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Get information on the current account's send quota.
    /// </summary>
    /// <returns>The send quota response data.</returns>
    public async Task<GetSendQuotaResponse> GetSendQuotaAsync()
    {
        var result = new GetSendQuotaResponse();
        try
        {
            var response = await _amazonSimpleEmailService.GetSendQuotaAsync(
                new GetSendQuotaRequest());
            result = response;
        }
        catch (Exception ex)
        {
            Console.WriteLine("GetSendQuotaAsync failed with exception: " +
ex.Message);
        }

        return result;
    }
```

- Pour plus de détails sur l'API, voir GetSendQuotala section Référence des AWS SDK for .NET API.

CLI

AWS CLI

Pour obtenir vos limites d'envoi Amazon SES

L'exemple suivant utilise la commande `get-send-quota` pour renvoyer vos limites d'envoi Amazon SES :

```
aws ses get-send-quota
```

Sortie :

```
{
   "Max24HourSend": 200.0,
```

```
    "SentLast24Hours": 1.0,
    "MaxSendRate": 1.0
}
```

Max24 HourSend est votre quota d'envoi, c'est-à-dire le nombre maximum d'e-mails que vous pouvez envoyer sur une période de 24 heures. Le quota d'envoi reflète une période glissante. Chaque fois que vous essayez d'envoyer un e-mail, Amazon SES vérifie le nombre d'e-mails que vous avez envoyés dans les dernières 24 heures. Tant que le nombre total d'e-mails que vous avez envoyés est inférieur à votre quota, votre demande d'envoi est acceptée et votre e-mail est envoyé.

SentLast24Hours est le nombre d'e-mails que vous avez envoyés au cours des 24 heures précédentes.

MaxSendRate est le nombre maximum d'e-mails que vous pouvez envoyer par seconde.

Notez que les limites d'envoi sont définies en fonction des destinataires et non pas des messages. Par exemple, un e-mail qui a 10 destinataires compte pour 10 dans votre quota d'envoi.

Pour plus d'informations, consultez Gestion de vos limites d'envoi Amazon SES dans le Guide du développeur Amazon Simple Email Service.

- Pour plus de détails sur l'API, voir GetSendQuotala section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cette commande renvoie les limites d'envoi actuelles de l'utilisateur.

```
Get-SESSendQuota
```

- Pour plus de détails sur l'API, consultez la section GetSendQuotaRéférence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`GetSendStatistics`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`GetSendStatistics`.

CLI

AWS CLI

Pour obtenir les statistiques d'envoi de votre Amazon SES

L'exemple suivant utilise la `get-send-statistics` commande pour renvoyer vos statistiques d'envoi Amazon SES.

```
aws ses get-send-statistics
```

Sortie :

```
{
   "SendDataPoints": [
       {
           "Complaints": 0,
           "Timestamp": "2013-06-12T19:32:00Z",
           "DeliveryAttempts": 2,
           "Bounces": 0,
           "Rejects": 0
       },
       {
           "Complaints": 0,
           "Timestamp": "2013-06-12T00:47:00Z",
           "DeliveryAttempts": 1,
           "Bounces": 0,
           "Rejects": 0
       }
   ]
}
```

Le résultat est une liste de points de données représentant les deux dernières semaines d'activité d'envoi. Chaque point de données de la liste contient des statistiques pour un intervalle de 15 minutes.

Dans cet exemple, il n'y a que deux points de données, car les seuls e-mails envoyés par l'utilisateur au cours des deux dernières semaines se situaient à deux intervalles de 15 minutes.

Pour plus d'informations, consultez la section Surveillance de vos statistiques d'utilisation d'Amazon SES dans le manuel Amazon Simple Email Service Developer Guide.

- Pour plus de détails sur l'API, voir GetSendStatisticsla section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cette commande renvoie les statistiques d'envoi de l'utilisateur. Le résultat est une liste de points de données représentant les deux dernières semaines d'activité d'envoi. Chaque point de données de la liste contient des statistiques pour un intervalle de 15 minutes.

```
Get-SESSendStatistic
```

- Pour plus de détails sur l'API, consultez la section GetSendStatisticsRéférence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`GetTemplate`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`GetTemplate`.

Les exemples d’actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l’exemple de code suivant :

- Vérifier une identité d'e-mail et envoyer des messages

C++

SDK pour C++

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
//! Get a template's attributes.
/*!
  \param templateName: The name for the template.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::getTemplate(const Aws::String &templateName,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::GetTemplateRequest getTemplateRequest;

    getTemplateRequest.SetTemplateName(templateName);

    Aws::SES::Model::GetTemplateOutcome outcome = sesClient.GetTemplate(
            getTemplateRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully got template." << std::endl;
    }

    else {
        std::cerr << "Error getting template. " <<
 outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Pour plus de détails sur l'API, voir GetTemplatela section Référence des AWS SDK for C++ API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { GetTemplateCommand } from "@aws-sdk/client-ses";
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";
import { sesClient } from "./libs/sesClient.js";

const TEMPLATE_NAME = getUniqueName("TemplateName");

const createGetTemplateCommand = (templateName) =>
  new GetTemplateCommand({ TemplateName: templateName });

const run = async () => {
  const getTemplateCommand = createGetTemplateCommand(TEMPLATE_NAME);

  try {
    return await sesClient.send(getTemplateCommand);
  } catch (caught) {
    if (caught instanceof Error && caught.name === "MessageRejected") {
      /** @type { import('@aws-sdk/client-ses').MessageRejected} */
      const messageRejectedError = caught;
      return messageRejectedError;
    }
    throw caught;
  }
};
```

- Pour plus de détails sur l'API, voir GetTemplatela section Référence des AWS SDK for JavaScript API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SesTemplate:
    """Encapsulates Amazon SES template functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client
        self.template = None
        self.template_tags = set()

    def _extract_tags(self, subject, text, html):
        """
        Extracts tags from a template as a set of unique values.

        :param subject: The subject of the email.
        :param text: The text version of the email.
        :param html: The html version of the email.
        """
        self.template_tags = set(re.findall(TEMPLATE_REGEX, subject + text +
 html))
        logger.info("Extracted template tags: %s", self.template_tags)


    def get_template(self, name):
        """
        Gets a previously created email template.

        :param name: The name of the template to retrieve.
        :return: The retrieved email template.
        """
        try:
```

```
            response = self.ses_client.get_template(TemplateName=name)
            self.template = response["Template"]
            logger.info("Got template %s.", name)
            self._extract_tags(
                self.template["SubjectPart"],
                self.template["TextPart"],
                self.template["HtmlPart"],
            )
        except ClientError:
            logger.exception("Couldn't get template %s.", name)
            raise
        else:
            return self.template
```

- Pour plus de détails sur l'API, consultez GetTemplatele AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`ListIdentities`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`ListIdentities`.

Les exemples d’actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans les exemples de code suivants :

- Copier les identités de domaine et d'e-mail dans les régions
- Vérifier une identité d'e-mail et envoyer des messages

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   /// <summary>
   /// Get the identities of a specified type for the current account.
   /// </summary>
   /// <param name="identityType">IdentityType to list.</param>
   /// <returns>The list of identities.</returns>
   public async Task<List<string>> ListIdentitiesAsync(IdentityType
identityType)
   {
       var result = new List<string>();
       try
       {
           var response = await _amazonSimpleEmailService.ListIdentitiesAsync(
               new ListIdentitiesRequest
               {
                   IdentityType = identityType
               });
           result = response.Identities;
       }
       catch (Exception ex)
       {
           Console.WriteLine("ListIdentitiesAsync failed with exception: " +
ex.Message);
       }

       return result;
   }
```

- Pour plus de détails sur l'API, voir ListIdentitiesla section Référence des AWS SDK for .NET API.

C++

SDK pour C++

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
//! List the identities associated with this account.
/*!
  \param identityType: The identity type enum. "NOT_SET" is a valid option.
  \param identities; A vector to receive the retrieved identities.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::listIdentities(Aws::SES::Model::IdentityType identityType,
                                 Aws::Vector<Aws::String> &identities,
                                 const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::ListIdentitiesRequest listIdentitiesRequest;

    if (identityType != Aws::SES::Model::IdentityType::NOT_SET) {
        listIdentitiesRequest.SetIdentityType(identityType);
    }

    Aws::String nextToken; // Used for paginated results.
    do {
        if (!nextToken.empty()) {
            listIdentitiesRequest.SetNextToken(nextToken);
        }
        Aws::SES::Model::ListIdentitiesOutcome outcome =
 sesClient.ListIdentities(
                listIdentitiesRequest);

        if (outcome.IsSuccess()) {
            const auto &retrievedIdentities =
 outcome.GetResult().GetIdentities();
            if (!retrievedIdentities.empty()) {
```

```
                identities.insert(identities.cend(),
 retrievedIdentities.cbegin(),
                                  retrievedIdentities.cend());
            }
            nextToken = outcome.GetResult().GetNextToken();
        }
        else {
            std::cout << "Error listing identities. " <<
 outcome.GetError().GetMessage()
                      << std::endl;
            return false;
        }
    } while (!nextToken.empty());

    return true;
}
```

- Pour plus de détails sur l'API, voir ListIdentitiesla section Référence des AWS SDK for C++ API.

CLI

AWS CLI

Pour répertorier toutes les identités (adresses e-mail et domaines) d'un AWS compte spécifique

L'exemple suivant utilise la commande `list-identities` pour répertorier toutes les identités soumises pour vérification auprès d'Amazon SES :

```
aws ses list-identities
```

Sortie :

```
{
    "Identities": [
      "user@example.com",
      "example.com"
    ]
```

```
}
```

La liste renvoyée contient toutes les identités, quel que soit le statut de vérification (vérifié, en attente de vérification, échec, etc.).

Dans cet exemple, les adresses e-mail et les domaines sont renvoyés car nous n'avons pas spécifié le paramètre identity-type.

Pour plus d'informations sur la vérification, consultez Vérification des adresses e-mail et des domaines dans Amazon SES dans le Guide du développeur Amazon Simple Email Service.

- Pour plus de détails sur l'API, voir ListIdentitiesla section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.ses.SesClient;
import software.amazon.awssdk.services.ses.model.ListIdentitiesResponse;
import software.amazon.awssdk.services.ses.model.SesException;
import java.io.IOException;
import java.util.List;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class ListIdentities {
```

```
    public static void main(String[] args) throws IOException {
        Region region = Region.US_WEST_2;
        SesClient client = SesClient.builder()
                .region(region)
                .build();

        listSESIdentities(client);
    }

    public static void listSESIdentities(SesClient client) {
        try {
            ListIdentitiesResponse identitiesResponse = client.listIdentities();
            List<String> identities = identitiesResponse.identities();
            for (String identity : identities) {
                System.out.println("The identity is " + identity);
            }

        } catch (SesException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
}
```

- Pour plus de détails sur l'API, voir ListIdentitiesla section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { ListIdentitiesCommand } from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";
```

```
const createListIdentitiesCommand = () =>
  new ListIdentitiesCommand({ IdentityType: "EmailAddress", MaxItems: 10 });

const run = async () => {
  const listIdentitiesCommand = createListIdentitiesCommand();

  try {
    return await sesClient.send(listIdentitiesCommand);
  } catch (err) {
    console.log("Failed to list identities.", err);
    return err;
  }
};
```

- Pour plus de détails sur l'API, voir ListIdentitiesla section Référence des AWS SDK for JavaScript API.

PowerShell

Outils pour PowerShell

Exemple 1 : Cette commande renvoie une liste contenant toutes les identités (adresses e-mail et domaines) d'un AWS compte spécifique, quel que soit le statut de vérification.

```
Get-SESIdentity
```

- Pour plus de détails sur l'API, consultez la section ListIdentitiesRéférence des AWS Tools for PowerShell applets de commande.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SesIdentity:
    """Encapsulates Amazon SES identity functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client


    def list_identities(self, identity_type, max_items):
        """
        Gets the identities of the specified type for the current account.

        :param identity_type: The type of identity to retrieve, such as
 EmailAddress.
        :param max_items: The maximum number of identities to retrieve.
        :return: The list of retrieved identities.
        """
        try:
            response = self.ses_client.list_identities(
                IdentityType=identity_type, MaxItems=max_items
            )
            identities = response["Identities"]
            logger.info("Got %s identities for the current account.",
 len(identities))
        except ClientError:
            logger.exception("Couldn't list identities for the current account.")
            raise
        else:
            return identities
```

- Pour plus de détails sur l'API, consultez ListIdentitiesle AWS manuel de référence de l'API SDK for Python (Boto3).

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
require "aws-sdk-ses"  # v2: require 'aws-sdk'

# Create client in us-west-2 region
# Replace us-west-2 with the AWS Region you're using for Amazon SES.
client = Aws::SES::Client.new(region: "us-west-2")

# Get up to 1000 identities
ids = client.list_identities({
  identity_type: "EmailAddress"
})

ids.identities.each do |email|
  attrs = client.get_identity_verification_attributes({
    identities: [email]
  })

  status = attrs.verification_attributes[email].verification_status

  # Display email addresses that have been verified
  if status == "Success"
    puts email
  end
end
```

- Pour plus de détails sur l'API, voir ListIdentitiesla section Référence des AWS SDK for Ruby API.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`ListReceiptFilters`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`ListReceiptFilters`.

C++

Kit de développement logiciel (SDK) for C++

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
//! List the receipt filters associated with this account.
/*!
  \param filters; A vector of "ReceiptFilter" to receive the retrieved filters.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool
AwsDoc::SES::listReceiptFilters(Aws::Vector<Aws::SES::Model::ReceiptFilter>
 &filters,
                                const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);
    Aws::SES::Model::ListReceiptFiltersRequest listReceiptFiltersRequest;

    Aws::SES::Model::ListReceiptFiltersOutcome outcome =
 sesClient.ListReceiptFilters(
            listReceiptFiltersRequest);
    if (outcome.IsSuccess()) {
        auto &retrievedFilters = outcome.GetResult().GetFilters();
        if (!retrievedFilters.empty()) {
            filters.insert(filters.cend(), retrievedFilters.cbegin(),
                           retrievedFilters.cend());
        }
    }
```

```
    else {
        std::cerr << "Error retrieving IP address filters: "
                  << outcome.GetError().GetMessage() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Pour plus de détails sur l'API, voir ListReceiptFilterslа section Référence des AWS SDK for C++ API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { ListReceiptFiltersCommand } from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";

const createListReceiptFiltersCommand = () => new ListReceiptFiltersCommand({});

const run = async () => {
  const listReceiptFiltersCommand = createListReceiptFiltersCommand();

  return await sesClient.send(listReceiptFiltersCommand);
};
```

- Pour plus de détails sur l'API, voir ListReceiptFilterslа section Référence des AWS SDK for JavaScript API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SesReceiptHandler:
    """Encapsulates Amazon SES receipt handling functions."""

    def __init__(self, ses_client, s3_resource):
        """
        :param ses_client: A Boto3 Amazon SES client.
        :param s3_resource: A Boto3 Amazon S3 resource.
        """
        self.ses_client = ses_client
        self.s3_resource = s3_resource


    def list_receipt_filters(self):
        """
        Gets the list of receipt filters for the current account.

        :return: The list of receipt filters.
        """
        try:
            response = self.ses_client.list_receipt_filters()
            filters = response["Filters"]
            logger.info("Got %s receipt filters.", len(filters))
        except ClientError:
            logger.exception("Couldn't get receipt filters.")
            raise
        else:
            return filters
```

- Pour plus de détails sur l'API, consultez ListReceiptFilterslе AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`ListTemplates`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`ListTemplates`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Vérifier une identité d'e-mail et envoyer des messages

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
/// <summary>
/// List email templates for the current account.
/// </summary>
/// <returns>A list of template metadata.</returns>
public async Task<List<TemplateMetadata>> ListEmailTemplatesAsync()
{
    var result = new List<TemplateMetadata>();
    try
    {
        var response = await _amazonSimpleEmailService.ListTemplatesAsync(
            new ListTemplatesRequest());
        result = response.TemplatesMetadata;
    }
    catch (Exception ex)
    {
```

```
            Console.WriteLine("ListEmailTemplatesAsync failed with exception: " +
ex.Message);
        }

        return result;
    }
```

- Pour plus de détails sur l'API, voir ListTemplatesla section Référence des AWS SDK for .NET API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.sesv2.SesV2Client;
import software.amazon.awssdk.services.sesv2.model.ListEmailTemplatesRequest;
import software.amazon.awssdk.services.sesv2.model.ListEmailTemplatesResponse;
import software.amazon.awssdk.services.sesv2.model.SesV2Exception;

public class ListTemplates {

    public static void main(String[] args) {
        Region region = Region.US_EAST_1;
        SesV2Client sesv2Client = SesV2Client.builder()
                .region(region)
                .build();

        listAllTemplates(sesv2Client);
    }

    public static void listAllTemplates(SesV2Client sesv2Client) {
        try {
```

```
            ListEmailTemplatesRequest templatesRequest =
 ListEmailTemplatesRequest.builder()
                    .pageSize(1)
                    .build();

            ListEmailTemplatesResponse response =
 sesv2Client.listEmailTemplates(templatesRequest);
            response.templatesMetadata()
                    .forEach(template -> System.out.println("Template name: " +
 template.templateName()));

        } catch (SesV2Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
}
```

- Pour plus de détails sur l'API, voir ListTemplatesla section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { ListTemplatesCommand } from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";

const createListTemplatesCommand = (maxItems) =>
  new ListTemplatesCommand({ MaxItems: maxItems });

const run = async () => {
  const listTemplatesCommand = createListTemplatesCommand(10);
```

```
  try {
    return await sesClient.send(listTemplatesCommand);
  } catch (err) {
    console.log("Failed to list templates.", err);
    return err;
  }
};
```

- Pour plus de détails sur l'API, voir ListTemplatesla section Référence des AWS SDK for JavaScript API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SesTemplate:
    """Encapsulates Amazon SES template functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client
        self.template = None
        self.template_tags = set()

    def _extract_tags(self, subject, text, html):
        """
        Extracts tags from a template as a set of unique values.

        :param subject: The subject of the email.
        :param text: The text version of the email.
        :param html: The html version of the email.
        """
```

```
        self.template_tags = set(re.findall(TEMPLATE_REGEX, subject + text +
html))
        logger.info("Extracted template tags: %s", self.template_tags)


    def list_templates(self):
        """
        Gets a list of all email templates for the current account.

        :return: The list of retrieved email templates.
        """
        try:
            response = self.ses_client.list_templates()
            templates = response["TemplatesMetadata"]
            logger.info("Got %s templates.", len(templates))
        except ClientError:
            logger.exception("Couldn't get templates.")
            raise
        else:
            return templates
```

- Pour plus de détails sur l'API, consultez ListTemplatesle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`SendBulkTemplatedEmail`** avec un AWS SDK ou une CLI

L'exemple de code suivant montre comment utiliser`SendBulkTemplatedEmail`.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { SendBulkTemplatedEmailCommand } from "@aws-sdk/client-ses";
import {
  getUniqueName,
  postfix,
} from "@aws-doc-sdk-examples/lib/utils/util-string.js";
import { sesClient } from "./libs/sesClient.js";

/**
 * Replace this with the name of an existing template.
 */
const TEMPLATE_NAME = getUniqueName("ReminderTemplate");

/**
 * Replace these with existing verified emails.
 */
const VERIFIED_EMAIL_1 = postfix(getUniqueName("Bilbo"), "@example.com");
const VERIFIED_EMAIL_2 = postfix(getUniqueName("Frodo"), "@example.com");

const USERS = [
  { firstName: "Bilbo", emailAddress: VERIFIED_EMAIL_1 },
  { firstName: "Frodo", emailAddress: VERIFIED_EMAIL_2 },
];

/**
 *
 * @param { { emailAddress: string, firstName: string }[] } users
 * @param { string } templateName the name of an existing template in SES
 * @returns { SendBulkTemplatedEmailCommand }
 */
const createBulkReminderEmailCommand = (users, templateName) => {
  return new SendBulkTemplatedEmailCommand({
    /**
```

```
     * Each 'Destination' uses a corresponding set of replacement data. We can
 map each user
     * to a 'Destination' and provide user specific replacement data to create
 personalized emails.
     *
     * Here's an example of how a template would be replaced with user data:
     * Template: <h1>Hello {{name}},</h1><p>Don't forget about the party gifts!</
p>
     * Destination 1: <h1>Hello Bilbo,</h1><p>Don't forget about the party gifts!
</p>
     * Destination 2: <h1>Hello Frodo,</h1><p>Don't forget about the party gifts!
</p>
     */
    Destinations: users.map((user) => ({
      Destination: { ToAddresses: [user.emailAddress] },
      ReplacementTemplateData: JSON.stringify({ name: user.firstName }),
    })),
    DefaultTemplateData: JSON.stringify({ name: "Shireling" }),
    Source: VERIFIED_EMAIL_1,
    Template: templateName,
  });
};

const run = async () => {
  const sendBulkTemplateEmailCommand = createBulkReminderEmailCommand(
    USERS,
    TEMPLATE_NAME,
  );
  try {
    return await sesClient.send(sendBulkTemplateEmailCommand);
  } catch (caught) {
    if (caught instanceof Error && caught.name === "MessageRejected") {
      /** @type { import('@aws-sdk/client-ses').MessageRejected} */
      const messageRejectedError = caught;
      return messageRejectedError;
    }
    throw caught;
  }
};
```

- Pour plus de détails sur l'API, voir SendBulkTemplatedEmailla section Référence des AWS SDK for JavaScript API.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`SendEmail`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`SendEmail`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Vérifier une identité d'e-mail et envoyer des messages

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
/// <summary>
///  Send an email by using Amazon SES.
/// </summary>
/// <param name="toAddresses">List of recipients.</param>
/// <param name="ccAddresses">List of cc recipients.</param>
/// <param name="bccAddresses">List of bcc recipients.</param>
/// <param name="bodyHtml">Body of the email in HTML.</param>
/// <param name="bodyText">Body of the email in plain text.</param>
/// <param name="subject">Subject line of the email.</param>
/// <param name="senderAddress">From address.</param>
/// <returns>The messageId of the email.</returns>
public async Task<string> SendEmailAsync(List<string> toAddresses,
    List<string> ccAddresses, List<string> bccAddresses,
    string bodyHtml, string bodyText, string subject, string senderAddress)
{
    var messageId = "";
```

```
        try
        {
            var response = await _amazonSimpleEmailService.SendEmailAsync(
                new SendEmailRequest
                {
                    Destination = new Destination
                    {
                        BccAddresses = bccAddresses,
                        CcAddresses = ccAddresses,
                        ToAddresses = toAddresses
                    },
                    Message = new Message
                    {
                        Body = new Body
                        {
                            Html = new Content
                            {
                                Charset = "UTF-8",
                                Data = bodyHtml
                            },
                            Text = new Content
                            {
                                Charset = "UTF-8",
                                Data = bodyText
                            }
                        },
                        Subject = new Content
                        {
                            Charset = "UTF-8",
                            Data = subject
                        }
                    },
                    Source = senderAddress
                });
            messageId = response.MessageId;
        }
        catch (Exception ex)
        {
            Console.WriteLine("SendEmailAsync failed with exception: " +
ex.Message);
        }

        return messageId;
    }
```

- Pour plus de détails sur l'API, voir SendEmailla section Référence des AWS SDK for .NET API.

C++

SDK pour C++

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
//! Send an email to a list of recipients.
/*!
  \param recipients; Vector of recipient email addresses.
  \param subject: Email subject.
  \param htmlBody: Email body as HTML. At least one body data is required.
  \param textBody: Email body as plain text. At least one body data is required.
  \param senderEmailAddress: Email address of sender. Ignored if empty string.
  \param ccAddresses: Vector of cc addresses. Ignored if empty.
  \param replyToAddress: Reply to email address. Ignored if empty string.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::sendEmail(const Aws::Vector<Aws::String> &recipients,
                            const Aws::String &subject,
                            const Aws::String &htmlBody,
                            const Aws::String &textBody,
                            const Aws::String &senderEmailAddress,
                            const Aws::Vector<Aws::String> &ccAddresses,
                            const Aws::String &replyToAddress,
                            const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::Destination destination;
    if (!ccAddresses.empty()) {
```

```
        destination.WithCcAddresses(ccAddresses);
    }
    if (!recipients.empty()) {
        destination.WithToAddresses(recipients);
    }

    Aws::SES::Model::Body message_body;
    if (!htmlBody.empty()) {
        message_body.SetHtml(

Aws::SES::Model::Content().WithCharset("UTF-8").WithData(htmlBody));
    }

    if (!textBody.empty()) {
        message_body.SetText(

Aws::SES::Model::Content().WithCharset("UTF-8").WithData(textBody));
    }

    Aws::SES::Model::Message message;
    message.SetBody(message_body);
    message.SetSubject(
            Aws::SES::Model::Content().WithCharset("UTF-8").WithData(subject));

    Aws::SES::Model::SendEmailRequest sendEmailRequest;
    sendEmailRequest.SetDestination(destination);
    sendEmailRequest.SetMessage(message);
    if (!senderEmailAddress.empty()) {
        sendEmailRequest.SetSource(senderEmailAddress);
    }
    if (!replyToAddress.empty()) {
        sendEmailRequest.AddReplyToAddresses(replyToAddress);
    }

    auto outcome = sesClient.SendEmail(sendEmailRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully sent message with ID "
                  << outcome.GetResult().GetMessageId()
                  << "." << std::endl;
    }
    else {
        std::cerr << "Error sending message. " << outcome.GetError().GetMessage()
                  << std::endl;
```

```
    }

    return outcome.IsSuccess();
}
```

- Pour plus de détails sur l'API, voir SendEmaillla section Référence des AWS SDK for C++ API.

CLI

AWS CLI

Pour envoyer un e-mail formaté à l'aide d'Amazon SES

L'exemple suivant utilise la commande `send-email` pour envoyer un e-mail formaté :

```
aws ses send-email --from sender@example.com --destination file://
destination.json --message file://message.json
```

Sortie :

```
{
   "MessageId": "EXAMPLEf3a5efcd1-51adec81-d2a4-4e3f-9fe2-5d85c1b23783-000000"
}
```

La destination et le message sont des structures de données JSON enregistrées dans des fichiers .json du répertoire actuel. Ces fichiers sont les suivants :

`destination.json`:

```
{
  "ToAddresses":  ["recipient1@example.com", "recipient2@example.com"],
  "CcAddresses":  ["recipient3@example.com"],
  "BccAddresses": []
}
```

`message.json`:

```
{
```

```
   "Subject": {
       "Data": "Test email sent using the AWS CLI",
       "Charset": "UTF-8"
   },
   "Body": {
       "Text": {
           "Data": "This is the message body in text format.",
           "Charset": "UTF-8"
       },
       "Html": {
           "Data": "This message body contains HTML formatting. It can, for
 example, contain links like this one: <a class=\"ulink\" href=\"http://
docs.aws.amazon.com/ses/latest/DeveloperGuide\" target=\"_blank\">Amazon SES
 Developer Guide</a>.",
           "Charset": "UTF-8"
       }
   }
}
```

Remplacez les adresses e-mail de l'expéditeur et du destinataire par celles que vous souhaitez utiliser. Notez que l'adresse e-mail de l'expéditeur doit être vérifiée avec Amazon SES. Jusqu'à ce que vous obteniez un accès en production pour Amazon SES, vous devez également vérifier l'adresse e-mail de chaque destinataire, sauf si le destinataire est le simulateur de boîte aux lettres Amazon SES. Pour plus d'informations sur la vérification, consultez Vérification des adresses e-mail et des domaines dans Amazon SES dans le Guide du développeur Amazon Simple Email Service.

L'ID du message dans la sortie indique que l'appel pour envoyer un e-mail a réussi.

Si vous ne recevez pas l'e-mail, vérifiez votre boîte de courrier indésirable.

Pour plus d'informations sur l'envoi d'un e-mail formaté, consultez Envoi d'e-mails formatés à l'aide de l'API Amazon SES dans le Guide du développeur Amazon Simple Email Service.

- Pour plus de détails sur l'API, voir SendEmaillla section Référence des AWS CLI commandes.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.ses.SesClient;
import software.amazon.awssdk.services.ses.model.Content;
import software.amazon.awssdk.services.ses.model.Destination;
import software.amazon.awssdk.services.ses.model.Message;
import software.amazon.awssdk.services.ses.model.Body;
import software.amazon.awssdk.services.ses.model.SendEmailRequest;
import software.amazon.awssdk.services.ses.model.SesException;

import javax.mail.MessagingException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class SendMessageEmailRequest {
    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <sender> <recipient> <subject>\s

                Where:
                    sender - An email address that represents the sender.\s
                    recipient -  An email address that represents the recipient.
\s
                    subject - The  subject line.\s
```

```
                """;

        if (args.length != 3) {
            System.out.println(usage);
            System.exit(1);
        }

        String sender = args[0];
        String recipient = args[1];
        String subject = args[2];

        Region region = Region.US_EAST_1;
        SesClient client = SesClient.builder()
                .region(region)
                .build();

        // The HTML body of the email.
        String bodyHTML = "<html>" + "<head></head>" + "<body>" + "<h1>Hello!</
h1>"
                + "<p> See the list of customers.</p>" + "</body>" + "</html>";

        try {
            send(client, sender, recipient, subject, bodyHTML);
            client.close();
            System.out.println("Done");

        } catch (MessagingException e) {
            e.getStackTrace();
        }
    }

    public static void send(SesClient client,
            String sender,
            String recipient,
            String subject,
            String bodyHTML) throws MessagingException {

        Destination destination = Destination.builder()
                .toAddresses(recipient)
                .build();

        Content content = Content.builder()
                .data(bodyHTML)
                .build();
```

```
        Content sub = Content.builder()
                .data(subject)
                .build();

        Body body = Body.builder()
                .html(content)
                .build();

        Message msg = Message.builder()
                .subject(sub)
                .body(body)
                .build();

        SendEmailRequest emailRequest = SendEmailRequest.builder()
                .destination(destination)
                .message(msg)
                .source(sender)
                .build();

        try {
            System.out.println("Attempting to send an email through Amazon SES "
 + "using the AWS SDK for Java...");
            client.sendEmail(emailRequest);

        } catch (SesException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
}

import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.ses.SesClient;
import javax.activation.DataHandler;
import javax.activation.DataSource;
import javax.mail.Message;
import javax.mail.MessagingException;
import javax.mail.Session;
import javax.mail.internet.AddressException;
import javax.mail.internet.InternetAddress;
import javax.mail.internet.MimeMessage;
import javax.mail.internet.MimeMultipart;
import javax.mail.internet.MimeBodyPart;
```

```
import javax.mail.util.ByteArrayDataSource;
import java.io.ByteArrayOutputStream;
import java.io.IOException;
import java.nio.ByteBuffer;
import java.nio.file.Files;
import java.util.Properties;
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.services.ses.model.SendRawEmailRequest;
import software.amazon.awssdk.services.ses.model.RawMessage;
import software.amazon.awssdk.services.ses.model.SesException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class SendMessageAttachment {
    public static void main(String[] args) throws IOException {
        final String usage = """

                Usage:
                    <sender> <recipient> <subject> <fileLocation>\s

                Where:
                    sender - An email address that represents the sender.\s
                    recipient -  An email address that represents the recipient.
\s
                    subject - The  subject line.\s
                    fileLocation - The location of a Microsoft Excel file to use
 as an attachment (C:/AWS/customers.xls).\s
                """;

        if (args.length != 4) {
            System.out.println(usage);
            System.exit(1);
        }

        String sender = args[0];
        String recipient = args[1];
```

```
        String subject = args[2];
        String fileLocation = args[3];

        // The email body for recipients with non-HTML email clients.
        String bodyText = "Hello,\r\n" + "Please see the attached file for a list
 "
                + "of customers to contact.";

        // The HTML body of the email.
        String bodyHTML = "<html>" + "<head></head>" + "<body>" + "<h1>Hello!</
h1>"
                + "<p>Please see the attached file for a " + "list of customers
 to contact.</p>" + "</body>"
                + "</html>";

        Region region = Region.US_WEST_2;
        SesClient client = SesClient.builder()
                .region(region)
                .build();

        try {
            sendemailAttachment(client, sender, recipient, subject, bodyText,
 bodyHTML, fileLocation);
            client.close();
            System.out.println("Done");

        } catch (IOException | MessagingException e) {
            e.getStackTrace();
        }
    }

    public static void sendemailAttachment(SesClient client,
            String sender,
            String recipient,
            String subject,
            String bodyText,
            String bodyHTML,
            String fileLocation) throws AddressException, MessagingException,
 IOException {

        java.io.File theFile = new java.io.File(fileLocation);
        byte[] fileContent = Files.readAllBytes(theFile.toPath());

        Session session = Session.getDefaultInstance(new Properties());
```

```
        // Create a new MimeMessage object.
        MimeMessage message = new MimeMessage(session);

        // Add subject, from and to lines.
        message.setSubject(subject, "UTF-8");
        message.setFrom(new InternetAddress(sender));
        message.setRecipients(Message.RecipientType.TO,
 InternetAddress.parse(recipient));

        // Create a multipart/alternative child container.
        MimeMultipart msgBody = new MimeMultipart("alternative");

        // Create a wrapper for the HTML and text parts.
        MimeBodyPart wrap = new MimeBodyPart();

        // Define the text part.
        MimeBodyPart textPart = new MimeBodyPart();
        textPart.setContent(bodyText, "text/plain; charset=UTF-8");

        // Define the HTML part.
        MimeBodyPart htmlPart = new MimeBodyPart();
        htmlPart.setContent(bodyHTML, "text/html; charset=UTF-8");

        // Add the text and HTML parts to the child container.
        msgBody.addBodyPart(textPart);
        msgBody.addBodyPart(htmlPart);

        // Add the child container to the wrapper object.
        wrap.setContent(msgBody);

        // Create a multipart/mixed parent container.
        MimeMultipart msg = new MimeMultipart("mixed");

        // Add the parent container to the message.
        message.setContent(msg);
        msg.addBodyPart(wrap);

        // Define the attachment.
        MimeBodyPart att = new MimeBodyPart();
        DataSource fds = new ByteArrayDataSource(fileContent,
                "application/vnd.openxmlformats-
officedocument.spreadsheetml.sheet");
        att.setDataHandler(new DataHandler(fds));
```

```
        String reportName = "WorkReport.xls";
        att.setFileName(reportName);

        // Add the attachment to the message.
        msg.addBodyPart(att);

        try {
            System.out.println("Attempting to send an email through Amazon SES "
 + "using the AWS SDK for Java...");

            ByteArrayOutputStream outputStream = new ByteArrayOutputStream();
            message.writeTo(outputStream);

            ByteBuffer buf = ByteBuffer.wrap(outputStream.toByteArray());

            byte[] arr = new byte[buf.remaining()];
            buf.get(arr);

            SdkBytes data = SdkBytes.fromByteArray(arr);
            RawMessage rawMessage = RawMessage.builder()
                    .data(data)
                    .build();

            SendRawEmailRequest rawEmailRequest = SendRawEmailRequest.builder()
                    .rawMessage(rawMessage)
                    .build();

            client.sendRawEmail(rawEmailRequest);

        } catch (SesException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        System.out.println("Email sent using SesClient with attachment");
    }
}
```

- Pour plus de détails sur l'API, voir SendEmailla section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { SendEmailCommand } from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";

const createSendEmailCommand = (toAddress, fromAddress) => {
  return new SendEmailCommand({
    Destination: {
      /* required */
      CcAddresses: [
        /* more items */
      ],
      ToAddresses: [
        toAddress,
        /* more To-email addresses */
      ],
    },
    Message: {
      /* required */
      Body: {
        /* required */
        Html: {
          Charset: "UTF-8",
          Data: "HTML_FORMAT_BODY",
        },
        Text: {
          Charset: "UTF-8",
          Data: "TEXT_FORMAT_BODY",
        },
      },
      Subject: {
        Charset: "UTF-8",
        Data: "EMAIL_SUBJECT",
      },
```

```
    },
    Source: fromAddress,
    ReplyToAddresses: [
      /* more items */
    ],
  });
};

const run = async () => {
  const sendEmailCommand = createSendEmailCommand(
    "recipient@example.com",
    "sender@example.com",
  );

  try {
    return await sesClient.send(sendEmailCommand);
  } catch (caught) {
    if (caught instanceof Error && caught.name === "MessageRejected") {
      /** @type { import('@aws-sdk/client-ses').MessageRejected} */
      const messageRejectedError = caught;
      return messageRejectedError;
    }
    throw caught;
  }
};
```

- Pour plus de détails sur l'API, voir SendEmailla section Référence des AWS SDK for JavaScript API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SesMailSender:
    """Encapsulates functions to send emails with Amazon SES."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client


    def send_email(self, source, destination, subject, text, html,
 reply_tos=None):
        """
        Sends an email.

        Note: If your account is in the Amazon SES  sandbox, the source and
        destination email accounts must both be verified.

        :param source: The source email account.
        :param destination: The destination email account.
        :param subject: The subject of the email.
        :param text: The plain text version of the body of the email.
        :param html: The HTML version of the body of the email.
        :param reply_tos: Email accounts that will receive a reply if the
 recipient
                          replies to the message.
        :return: The ID of the message, assigned by Amazon SES.
        """
        send_args = {
            "Source": source,
            "Destination": destination.to_service_format(),
            "Message": {
                "Subject": {"Data": subject},
                "Body": {"Text": {"Data": text}, "Html": {"Data": html}},
            },
        }
        if reply_tos is not None:
            send_args["ReplyToAddresses"] = reply_tos
        try:
            response = self.ses_client.send_email(**send_args)
            message_id = response["MessageId"]
            logger.info(
```

```
                "Sent mail %s from %s to %s.", message_id, source,
destination.tos
            )
        except ClientError:
            logger.exception(
                "Couldn't send mail from %s to %s.", source, destination.tos
            )
            raise
        else:
            return message_id
```

- Pour plus de détails sur l'API, consultez SendEmaille AWS manuel de référence de l'API SDK for Python (Boto3).

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
require "aws-sdk-ses"  # v2: require 'aws-sdk'

# Replace sender@example.com with your "From" address.
# This address must be verified with Amazon SES.
sender = "sender@example.com"

# Replace recipient@example.com with a "To" address. If your account
# is still in the sandbox, this address must be verified.
recipient = "recipient@example.com"

# Specify a configuration set. To use a configuration
# set, uncomment the next line and line 74.
#   configsetname = "ConfigSet"
```

```
# The subject line for the email.
subject = "Amazon SES test (AWS SDK for Ruby)"

# The HTML body of the email.
htmlbody =
  "<h1>Amazon SES test (AWS SDK for Ruby)</h1>"\
  '<p>This email was sent with <a href="https://aws.amazon.com/ses/">'\
  'Amazon SES</a> using the <a href="https://aws.amazon.com/sdk-for-ruby/">'\
  "AWS SDK for Ruby</a>."

# The email body for recipients with non-HTML email clients.
textbody = "This email was sent with Amazon SES using the AWS SDK for Ruby."

# Specify the text encoding scheme.
encoding = "UTF-8"

# Create a new SES client in the us-west-2 region.
# Replace us-west-2 with the AWS Region you're using for Amazon SES.
ses = Aws::SES::Client.new(region: "us-west-2")

# Try to send the email.
begin
  # Provide the contents of the email.
  ses.send_email(
    destination: {
      to_addresses: [
        recipient
      ]
    },
    message: {
      body: {
        html: {
          charset: encoding,
          data: htmlbody
        },
        text: {
          charset: encoding,
          data: textbody
        }
      },
      subject: {
        charset: encoding,
        data: subject
      }
```

```
    },
    source: sender,
    # Uncomment the following line to use a configuration set.
    # configuration_set_name: configsetname,
    )

  puts "Email sent to " + recipient

# If something goes wrong, display an error message.
rescue Aws::SES::Errors::ServiceError => error
  puts "Email not sent. Error message: #{error}"
end
```

- Pour plus de détails sur l'API, voir SendEmailla section Référence des AWS SDK for Ruby API.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`SendRawEmail`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`SendRawEmail`.

CLI

AWS CLI

Pour envoyer un e-mail brut à l'aide d'Amazon SES

L'exemple suivant utilise la commande `send-raw-email` pour envoyer un e-mail avec une pièce jointe TXT :

```
aws ses send-raw-email --raw-message file://message.json
```

Sortie :

```
{
   "MessageId": "EXAMPLEf3f73d99b-c63fb06f-d263-41f8-a0fb-d0dc67d56c07-000000"
```

```
}
```

Le message brut est une structure de données JSON enregistrée dans un fichier nommé `message.json` dans le répertoire actuel. Il contient les éléments suivants :

```
{
   "Data": "From: sender@example.com\nTo: recipient@example.com\nSubject:
 Test email sent using the AWS CLI (contains an attachment)\nMIME-Version:
 1.0\nContent-type: Multipart/Mixed; boundary=\"NextPart\"\n\n--NextPart
\nContent-Type: text/plain\n\nThis is the message body.\n\n--NextPart\nContent-
Type: text/plain;\nContent-Disposition: attachment; filename=\"attachment.txt\"\n
\nThis is the text in the attachment.\n\n--NextPart--"
}
```

Comme vous pouvez le constater, « Data » est une longue chaîne contenant l'intégralité du contenu de l'e-mail brut au format MIME, y compris une pièce jointe appelée attachment.txt.

Remplacez sender@example.com et recipient@example.com par les adresses que vous souhaitez utiliser. Notez que l'adresse e-mail de l'expéditeur doit être vérifiée avec Amazon SES. Jusqu'à ce que vous obteniez un accès en production pour Amazon SES, vous devez également vérifier l'adresse e-mail du destinataire, sauf si le destinataire est le simulateur de boîte aux lettres Amazon SES. Pour plus d'informations sur la vérification, consultez Vérification des adresses e-mail et des domaines dans Amazon SES dans le Guide du développeur Amazon Simple Email Service.

L'ID du message dans la sortie indique que l'appel send-raw-email a réussi.

Si vous ne recevez pas l'e-mail, vérifiez votre boîte de courrier indésirable.

Pour plus d'informations sur l'envoi d'un e-mail brut, consultez Envoi d'e-mails bruts à l'aide de l'API Amazon SES dans le Guide du développeur Amazon Simple Email Service.

- Pour plus de détails sur l'API, voir SendRawEmailla section Référence des AWS CLI commandes.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Utilisez nodemailer pour envoyer un e-mail avec une pièce jointe.

```
import sesClientModule from "@aws-sdk/client-ses";
/**
 * nodemailer wraps the SES SDK and calls SendRawEmail. Use this for more
 advanced
 * functionality like adding attachments to your email.
 *
 * https://nodemailer.com/transports/ses/
 */
import nodemailer from "nodemailer";

/**
 * @param {string} from An Amazon SES verified email address.
 * @param {*} to An Amazon SES verified email address.
 */
export const sendEmailWithAttachments = (
  from = "from@example.com",
  to = "to@example.com",
) => {
  const ses = new sesClientModule.SESClient({});
  const transporter = nodemailer.createTransport({
    SES: { ses, aws: sesClientModule },
  });

  return new Promise((resolve, reject) => {
    transporter.sendMail(
      {
        from,
        to,
        subject: "Hello World",
        text: "Greetings from Amazon SES!",
        attachments: [{ content: "Hello World!", filename: "hello.txt" }],
```

```
      },
      (err, info) => {
        if (err) {
          reject(err);
        } else {
          resolve(info);
        }
      },
    );
  });
};
```

- Pour plus de détails sur l'API, voir SendRawEmailla section Référence des AWS SDK for JavaScript API.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`SendTemplatedEmail`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`SendTemplatedEmail`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Vérifier une identité d'e-mail et envoyer des messages

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   /// <summary>
   /// Send an email using a template.
   /// </summary>
   /// <param name="sender">Address of the sender.</param>
   /// <param name="recipients">Addresses of the recipients.</param>
   /// <param name="templateName">Name of the email template.</param>
   /// <param name="templateDataObject">Data for the email template.</param>
   /// <returns>The messageId of the email.</returns>
   public async Task<string> SendTemplateEmailAsync(string sender, List<string>
recipients,
       string templateName, object templateDataObject)
   {
       var messageId = "";
       try
       {
           // Template data should be serialized JSON from either a class or a
dynamic object.
           var templateData = JsonSerializer.Serialize(templateDataObject);

           var response = await
_amazonSimpleEmailService.SendTemplatedEmailAsync(
               new SendTemplatedEmailRequest
               {
                   Source = sender,
                   Destination = new Destination
                   {
                       ToAddresses = recipients
                   },
                   Template = templateName,
                   TemplateData = templateData
               });
           messageId = response.MessageId;
       }
       catch (Exception ex)
       {
           Console.WriteLine("SendTemplateEmailAsync failed with exception: " +
ex.Message);
       }

       return messageId;
   }
```

- Pour plus de détails sur l'API, voir SendTemplatedEmailla section Référence des AWS SDK for .NET API.

C++

SDK pour C++

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
//! Send a templated email to a list of recipients.
/*!
  \param recipients; Vector of recipient email addresses.
  \param templateName: The name of the template to use.
  \param templateData: Map of key-value pairs for replacing text in template.
  \param senderEmailAddress: Email address of sender. Ignored if empty string.
  \param ccAddresses: Vector of cc addresses. Ignored if empty.
  \param replyToAddress: Reply to email address. Ignored if empty string.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::sendTemplatedEmail(const Aws::Vector<Aws::String> &recipients,
                                     const Aws::String &templateName,
                                     const Aws::Map<Aws::String, Aws::String>
 &templateData,
                                     const Aws::String &senderEmailAddress,
                                     const Aws::Vector<Aws::String> &ccAddresses,
                                     const Aws::String &replyToAddress,
                                     const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::Destination destination;
    if (!ccAddresses.empty()) {
        destination.WithCcAddresses(ccAddresses);
    }
```

```
    if (!recipients.empty()) {
        destination.WithToAddresses(recipients);
    }

    Aws::SES::Model::SendTemplatedEmailRequest sendTemplatedEmailRequest;
    sendTemplatedEmailRequest.SetDestination(destination);
    sendTemplatedEmailRequest.SetTemplate(templateName);

    std::ostringstream templateDataStream;
    templateDataStream << "{";
    size_t dataCount = 0;
    for (auto &pair: templateData) {
        templateDataStream << "\"" << pair.first << "\":\"" << pair.second <<
"\"";
        dataCount++;
        if (dataCount < templateData.size()) {
            templateDataStream << ",";
        }
    }
    templateDataStream << "}";

    sendTemplatedEmailRequest.SetTemplateData(templateDataStream.str());

    if (!senderEmailAddress.empty()) {
        sendTemplatedEmailRequest.SetSource(senderEmailAddress);
    }
    if (!replyToAddress.empty()) {
        sendTemplatedEmailRequest.AddReplyToAddresses(replyToAddress);
    }

    auto outcome = sesClient.SendTemplatedEmail(sendTemplatedEmailRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully sent templated message with ID "
                  << outcome.GetResult().GetMessageId()
                  << "." << std::endl;
    }
    else {
        std::cerr << "Error sending templated message. "
                  << outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
```

```
}
```

- Pour plus de détails sur l'API, voir SendTemplatedEmaillla section Référence des AWS SDK for C++ API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.sesv2.model.Destination;
import software.amazon.awssdk.services.sesv2.model.EmailContent;
import software.amazon.awssdk.services.sesv2.model.SendEmailRequest;
import software.amazon.awssdk.services.sesv2.model.SesV2Exception;
import software.amazon.awssdk.services.sesv2.SesV2Client;
import software.amazon.awssdk.services.sesv2.model.Template;

/**
 * Before running this AWS SDK for Java (v2) example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * Also, make sure that you create a template. See the following documentation
 * topic:
 *
 * https://docs.aws.amazon.com/ses/latest/dg/send-personalized-email-api.html
 */

public class SendEmailTemplate {
    public static void main(String[] args) {
```

```
        final String usage = """

                Usage:
                    <template> <sender> <recipient>\s

                Where:
                    template - The name of the email template.
                    sender - An email address that represents the sender.\s
                    recipient - An email address that represents the recipient.\s
                """;

        if (args.length != 3) {
            System.out.println(usage);
            System.exit(1);
        }

        String templateName = args[0];
        String sender = args[1];
        String recipient = args[2];
        Region region = Region.US_EAST_1;
        SesV2Client sesv2Client = SesV2Client.builder()
                .region(region)
                .build();

        send(sesv2Client, sender, recipient, templateName);
    }

    public static void send(SesV2Client client, String sender, String recipient,
String templateName) {
        Destination destination = Destination.builder()
                .toAddresses(recipient)
                .build();

        /*
         * Specify both name and favorite animal (favoriteanimal) in your code
when
         * defining the Template object.
         * If you don't specify all the variables in the template, Amazon SES
doesn't
         * send the email.
         */
        Template myTemplate = Template.builder()
                .templateName(templateName)
                .templateData("{\n" +
```

```
                        "  \"name\": \"Jason\"\n," +
                        "  \"favoriteanimal\": \"Cat\"\n" +
                        "}")
                .build();

        EmailContent emailContent = EmailContent.builder()
                .template(myTemplate)
                .build();

        SendEmailRequest emailRequest = SendEmailRequest.builder()
                .destination(destination)
                .content(emailContent)
                .fromEmailAddress(sender)
                .build();

        try {
            System.out.println("Attempting to send an email based on a template
 using the AWS SDK for Java (v2)...");
            client.sendEmail(emailRequest);
            System.out.println("email based on a template was sent");

        } catch (SesV2Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
}
```

- Pour plus de détails sur l'API, voir SendTemplatedEmailla section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { SendTemplatedEmailCommand } from "@aws-sdk/client-ses";
import {
  getUniqueName,
  postfix,
} from "@aws-doc-sdk-examples/lib/utils/util-string.js";
import { sesClient } from "./libs/sesClient.js";

/**
 * Replace this with the name of an existing template.
 */
const TEMPLATE_NAME = getUniqueName("ReminderTemplate");

/**
 * Replace these with existing verified emails.
 */
const VERIFIED_EMAIL = postfix(getUniqueName("Bilbo"), "@example.com");

const USER = { firstName: "Bilbo", emailAddress: VERIFIED_EMAIL };

/**
 *
 * @param { { emailAddress: string, firstName: string } } user
 * @param { string } templateName - The name of an existing template in Amazon
 SES.
 * @returns { SendTemplatedEmailCommand }
 */
const createReminderEmailCommand = (user, templateName) => {
  return new SendTemplatedEmailCommand({
    /**
     * Here's an example of how a template would be replaced with user data:
     * Template: <h1>Hello {{contact.firstName}},</h1><p>Don't forget about the
 party gifts!</p>
     * Destination: <h1>Hello Bilbo,</h1><p>Don't forget about the party gifts!</
p>
     */
    Destination: { ToAddresses: [user.emailAddress] },
    TemplateData: JSON.stringify({ contact: { firstName: user.firstName } }),
    Source: VERIFIED_EMAIL,
    Template: templateName,
  });
};

const run = async () => {
```

```
  const sendReminderEmailCommand = createReminderEmailCommand(
    USER,
    TEMPLATE_NAME,
  );
  try {
    return await sesClient.send(sendReminderEmailCommand);
  } catch (caught) {
    if (caught instanceof Error && caught.name === "MessageRejected") {
      /** @type { import('@aws-sdk/client-ses').MessageRejected} */
      const messageRejectedError = caught;
      return messageRejectedError;
    }
    throw caught;
  }
};
```

- Pour plus de détails sur l'API, voir SendTemplatedEmaillla section Référence des AWS SDK for JavaScript API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SesMailSender:
    """Encapsulates functions to send emails with Amazon SES."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client


    def send_templated_email(
```

```
        self, source, destination, template_name, template_data, reply_tos=None
    ):
        """
        Sends an email based on a template. A template contains replaceable tags
        each enclosed in two curly braces, such as {{name}}. The template data
passed
        in this function contains key-value pairs that define the values to
insert
        in place of the template tags.

        Note: If your account is in the Amazon SES  sandbox, the source and
        destination email accounts must both be verified.

        :param source: The source email account.
        :param destination: The destination email account.
        :param template_name: The name of a previously created template.
        :param template_data: JSON-formatted key-value pairs of replacement
values
                              that are inserted in the template before it is
sent.
        :return: The ID of the message, assigned by Amazon SES.
        """
        send_args = {
            "Source": source,
            "Destination": destination.to_service_format(),
            "Template": template_name,
            "TemplateData": json.dumps(template_data),
        }
        if reply_tos is not None:
            send_args["ReplyToAddresses"] = reply_tos
        try:
            response = self.ses_client.send_templated_email(**send_args)
            message_id = response["MessageId"]
            logger.info(
                "Sent templated mail %s from %s to %s.",
                message_id,
                source,
                destination.tos,
            )
        except ClientError:
            logger.exception(
                "Couldn't send templated mail from %s to %s.", source,
destination.tos
            )
```

```
            raise
        else:
            return message_id
```

- Pour plus de détails sur l'API, consultez SendTemplatedEmaille AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`UpdateTemplate`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`UpdateTemplate`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Vérifier une identité d'e-mail et envoyer des messages

C++

SDK pour C++

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
//! Update an Amazon Simple Email Service (Amazon SES) template.
/*!
  \param templateName: The name of the template.
  \param htmlPart: The HTML body of the email.
  \param subjectPart: The subject line of the email.
```

```
  \param textPart: The plain text version of the email.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::updateTemplate(const Aws::String &templateName,
                                 const Aws::String &htmlPart,
                                 const Aws::String &subjectPart,
                                 const Aws::String &textPart,
                                 const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::Template templateValues;

    templateValues.SetTemplateName(templateName);
    templateValues.SetSubjectPart(subjectPart);
    templateValues.SetHtmlPart(htmlPart);
    templateValues.SetTextPart(textPart);

    Aws::SES::Model::UpdateTemplateRequest updateTemplateRequest;
    updateTemplateRequest.SetTemplate(templateValues);

    Aws::SES::Model::UpdateTemplateOutcome outcome =
 sesClient.UpdateTemplate(updateTemplateRequest);

    if (outcome.IsSuccess()) {
        std::cout << "Successfully updated template." << std::endl;
    } else {
        std::cerr << "Error updating template. " <<
 outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Pour plus de détails sur l'API, voir UpdateTemplatela section Référence des AWS SDK for C ++ API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { UpdateTemplateCommand } from "@aws-sdk/client-ses";
import { getUniqueName } from "@aws-doc-sdk-examples/lib/utils/util-string.js";
import { sesClient } from "./libs/sesClient.js";

const TEMPLATE_NAME = getUniqueName("TemplateName");
const HTML_PART = "<h1>Hello, World!</h1>";

const createUpdateTemplateCommand = () => {
  return new UpdateTemplateCommand({
    Template: {
      TemplateName: TEMPLATE_NAME,
      HtmlPart: HTML_PART,
      SubjectPart: "Example",
      TextPart: "Updated template text.",
    },
  });
};

const run = async () => {
  const updateTemplateCommand = createUpdateTemplateCommand();

  try {
    return await sesClient.send(updateTemplateCommand);
  } catch (err) {
    console.log("Failed to update template.", err);
    return err;
  }
};
```

- Pour plus de détails sur l'API, voir UpdateTemplatela section Référence des AWS SDK for JavaScript API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SesTemplate:
    """Encapsulates Amazon SES template functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client
        self.template = None
        self.template_tags = set()

    def _extract_tags(self, subject, text, html):
        """
        Extracts tags from a template as a set of unique values.

        :param subject: The subject of the email.
        :param text: The text version of the email.
        :param html: The html version of the email.
        """
        self.template_tags = set(re.findall(TEMPLATE_REGEX, subject + text +
 html))
        logger.info("Extracted template tags: %s", self.template_tags)


    def update_template(self, name, subject, text, html):
        """
        Updates a previously created email template.

        :param name: The name of the template.
        :param subject: The subject of the email.
        :param text: The plain text version of the email.
        :param html: The HTML version of the email.
```

```
        """
        try:
            template = {
                "TemplateName": name,
                "SubjectPart": subject,
                "TextPart": text,
                "HtmlPart": html,
            }
            self.ses_client.update_template(Template=template)
            logger.info("Updated template %s.", name)
            self.template = template
            self._extract_tags(subject, text, html)
        except ClientError:
            logger.exception("Couldn't update template %s.", name)
            raise
```

- Pour plus de détails sur l'API, consultez UpdateTemplatele AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`VerifyDomainIdentity`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`VerifyDomainIdentity`.

Les exemples d’actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans les exemples de code suivants :

- Copier les identités de domaine et d'e-mail dans les régions
- Vérifier une identité d'e-mail et envoyer des messages

CLI

AWS CLI

Pour vérifier un domaine avec Amazon SES

L'exemple suivant utilise la commande `verify-domain-identity` pour vérifier un domaine :

```
aws ses verify-domain-identity --domain example.com
```

Sortie :

```
{
   "VerificationToken": "eoEmxw+YaYhb3h3iVJHuXMJXqeu1q1/wwmvjuEXAMPLE"
}
```

Pour terminer la vérification du domaine, vous devez ajouter un enregistrement TXT avec le jeton de vérification renvoyé aux paramètres DNS de votre domaine. Pour plus d'informations, consultez Vérification des domaines dans Amazon SES dans le Guide du développeur Amazon Simple Email Service.

- Pour plus de détails sur l'API, voir VerifyDomainIdentityla section Référence des AWS CLI commandes.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import { VerifyDomainIdentityCommand } from "@aws-sdk/client-ses";
import {
  getUniqueName,
  postfix,
} from "@aws-doc-sdk-examples/lib/utils/util-string.js";
```

```
import { sesClient } from "./libs/sesClient.js";

/**
 * You must have access to the domain's DNS settings to complete the
 * domain verification process.
 */
const DOMAIN_NAME = postfix(getUniqueName("Domain"), ".example.com");

const createVerifyDomainIdentityCommand = () => {
  return new VerifyDomainIdentityCommand({ Domain: DOMAIN_NAME });
};

const run = async () => {
  const VerifyDomainIdentityCommand = createVerifyDomainIdentityCommand();

  try {
    return await sesClient.send(VerifyDomainIdentityCommand);
  } catch (err) {
    console.log("Failed to verify domain.", err);
    return err;
  }
};
```

- Pour plus de détails sur l'API, voir VerifyDomainIdentityla section Référence des AWS SDK for JavaScript API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SesIdentity:
    """Encapsulates Amazon SES identity functions."""

    def __init__(self, ses_client):
```

```
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client


    def verify_domain_identity(self, domain_name):
        """
        Starts verification of a domain identity. To complete verification, you
 must
        create a TXT record with a specific format through your DNS provider.

        For more information, see *Verifying a domain with Amazon SES* in the
        Amazon SES documentation:
            https://docs.aws.amazon.com/ses/latest/DeveloperGuide/verify-domain-
procedure.html

        :param domain_name: The name of the domain to verify.
        :return: The token to include in the TXT record with your DNS provider.
        """
        try:
            response = self.ses_client.verify_domain_identity(Domain=domain_name)
            token = response["VerificationToken"]
            logger.info("Got domain verification token for %s.", domain_name)
        except ClientError:
            logger.exception("Couldn't verify domain %s.", domain_name)
            raise
        else:
            return token
```

- Pour plus de détails sur l'API, consultez VerifyDomainIdentityle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`VerifyEmailIdentity`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`VerifyEmailIdentity`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans les exemples de code suivants :

- Copier les identités de domaine et d'e-mail dans les régions
- Vérifier une identité d'e-mail et envoyer des messages

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   /// <summary>
   /// Starts verification of an email identity. This request sends an email
   /// from Amazon SES to the specified email address. To complete
   /// verification, follow the instructions in the email.
   /// </summary>
   /// <param name="recipientEmailAddress">Email address to verify.</param>
   /// <returns>True if successful.</returns>
   public async Task<bool> VerifyEmailIdentityAsync(string
recipientEmailAddress)
   {
       var success = false;
       try
       {
           var response = await
_amazonSimpleEmailService.VerifyEmailIdentityAsync(
               new VerifyEmailIdentityRequest
               {
                   EmailAddress = recipientEmailAddress
               });

           success = response.HttpStatusCode == HttpStatusCode.OK;
       }
       catch (Exception ex)
```

```
        {
            Console.WriteLine("VerifyEmailIdentityAsync failed with exception: "
 + ex.Message);
        }

        return success;
    }
```

- Pour plus de détails sur l'API, voir VerifyEmailIdentityla section Référence des AWS SDK for .NET API.

C++

SDK pour C++

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
//! Add an email address to the list of identities associated with this account
 and
//! initiate verification.
/*!
  \param emailAddress; The email address to add.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SES::verifyEmailIdentity(const Aws::String &emailAddress,
                         const Aws::Client::ClientConfiguration
 &clientConfiguration)
{
    Aws::SES::SESClient sesClient(clientConfiguration);

    Aws::SES::Model::VerifyEmailIdentityRequest verifyEmailIdentityRequest;

    verifyEmailIdentityRequest.SetEmailAddress(emailAddress);
```

```
    Aws::SES::Model::VerifyEmailIdentityOutcome outcome =
 sesClient.VerifyEmailIdentity(verifyEmailIdentityRequest);

    if (outcome.IsSuccess())
    {
        std::cout << "Email verification initiated." << std::endl;
    }

    else
    {
        std::cerr << "Error initiating email verification. " <<
 outcome.GetError().GetMessage()
                  << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Pour plus de détails sur l'API, voir VerifyEmailIdentityla section Référence des AWS SDK for C++ API.

CLI

AWS CLI

Pour vérifier une adresse e-mail avec Amazon SES

L'exemple suivant utilise la commande `verify-email-identity` pour vérifier une adresse e-mail :

```
aws ses verify-email-identity --email-address user@example.com
```

Avant de pouvoir envoyer un e-mail avec Amazon SES, vous devez vérifier l'adresse ou le domaine à partir desquels vous envoyez l'e-mail afin de prouver que vous en êtes le propriétaire. Si vous n'avez pas encore l'accès en production, vous devez également vérifier toutes les adresses e-mail des destinataires, à l'exception de celles fournies par le simulateur de boîte aux lettres Amazon SES.

Après avoir été verify-email-identity appelée, l'adresse e-mail recevra un e-mail de vérification. L'utilisateur doit cliquer sur le lien disponible dans l'e-mail pour terminer le processus de vérification.

Pour plus d'informations, consultez Vérification des adresses e-mail dans Amazon SES dans le Guide du développeur Amazon Simple Email Service.

- Pour plus de détails sur l'API, voir VerifyEmailIdentityla section Référence des AWS CLI commandes.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
// Import required AWS SDK clients and commands for Node.js
import { VerifyEmailIdentityCommand } from "@aws-sdk/client-ses";
import { sesClient } from "./libs/sesClient.js";

const EMAIL_ADDRESS = "name@example.com";

const createVerifyEmailIdentityCommand = (emailAddress) => {
  return new VerifyEmailIdentityCommand({ EmailAddress: emailAddress });
};

const run = async () => {
  const verifyEmailIdentityCommand =
    createVerifyEmailIdentityCommand(EMAIL_ADDRESS);
  try {
    return await sesClient.send(verifyEmailIdentityCommand);
  } catch (err) {
    console.log("Failed to verify email identity.", err);
    return err;
  }
};
```

- Pour plus de détails sur l'API, voir VerifyEmailIdentityla section Référence des AWS SDK for JavaScript API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SesIdentity:
    """Encapsulates Amazon SES identity functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client


    def verify_email_identity(self, email_address):
        """
        Starts verification of an email identity. This function causes an email
        to be sent to the specified email address from Amazon SES. To complete
        verification, follow the instructions in the email.

        :param email_address: The email address to verify.
        """
        try:
            self.ses_client.verify_email_identity(EmailAddress=email_address)
            logger.info("Started verification of %s.", email_address)
        except ClientError:
            logger.exception("Couldn't start verification of %s.", email_address)
            raise
```

- Pour plus de détails sur l'API, consultez VerifyEmailIdentityle AWS manuel de référence de l'API SDK for Python (Boto3).

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
require "aws-sdk-ses"  # v2: require 'aws-sdk'

# Replace recipient@example.com with a "To" address.
recipient = "recipient@example.com"

# Create a new SES resource in the us-west-2 region.
# Replace us-west-2 with the AWS Region you're using for Amazon SES.
ses = Aws::SES::Client.new(region: "us-west-2")

# Try to verify email address.
begin
  ses.verify_email_identity({
    email_address: recipient
  })

  puts "Email sent to " + recipient

# If something goes wrong, display an error message.
rescue Aws::SES::Errors::ServiceError => error
  puts "Email not sent. Error message: #{error}"
end
```

- Pour plus de détails sur l'API, voir VerifyEmailIdentityla section Référence des AWS SDK for Ruby API.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Scénarios pour Amazon SES utilisant des AWS kits de développement logiciel

Les exemples de code suivants vous montrent comment implémenter des scénarios courants dans Amazon SES à l'aide de AWS kits SDK. Ces scénarios vous montrent comment accomplir des tâches spécifiques en appelant plusieurs fonctions dans Amazon SES. Chaque scénario inclut un lien vers GitHub, où vous pouvez trouver des instructions sur la façon de configurer et d'exécuter le code.

Exemples

- Copiez les adresses e-mail et les identités de domaine Amazon SES d'une AWS région à l'autre à l'aide d'un AWS SDK
- Générer des informations d'identification pour vous connecter à un point de terminaison d'un SMTP Amazon SES
- Vérifiez une identité e-mail et envoyez des messages avec Amazon SES à l'aide d'un AWS SDK

Copiez les adresses e-mail et les identités de domaine Amazon SES d'une AWS région à l'autre à l'aide d'un AWS SDK

L'exemple de code suivant montre comment copier les adresses e-mail et les identités de domaine Amazon SES d'une AWS région à l'autre. Lorsque les identités de domaine sont gérées par Route 53, les registres de vérification sont copiés dans le domaine de la Région de destination.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import argparse
```

```
import json
import logging
from pprint import pprint
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)


def get_identities(ses_client):
    """
    Gets the identities for the current Region. The Region is specified in the
    Boto3 Amazon SES client object.

    :param ses_client: A Boto3 Amazon SES client.
    :return: The list of email identities and the list of domain identities.
    """
    email_identities = []
    domain_identities = []
    try:
        identity_paginator = ses_client.get_paginator("list_identities")
        identity_iterator = identity_paginator.paginate(
            PaginationConfig={"PageSize": 20}
        )
        for identity_page in identity_iterator:
            for identity in identity_page["Identities"]:
                if "@" in identity:
                    email_identities.append(identity)
                else:
                    domain_identities.append(identity)
        logger.info(
            "Found %s email and %s domain identities.",
            len(email_identities),
            len(domain_identities),
        )
    except ClientError:
        logger.exception("Couldn't get identities.")
        raise
    else:
        return email_identities, domain_identities


def verify_emails(email_list, ses_client):
    """
```

```
    Starts verification of a list of email addresses. Verification causes an
 email
    to be sent to each address. To complete verification, the recipient must
 follow
    the instructions in the email.

    :param email_list: The list of email addresses to verify.
    :param ses_client: A Boto3 Amazon SES client.
    :return: The list of emails that were successfully submitted for
 verification.
    """
    verified_emails = []
    for email in email_list:
        try:
            ses_client.verify_email_identity(EmailAddress=email)
            verified_emails.append(email)
            logger.info("Started verification of %s.", email)
        except ClientError:
            logger.warning("Couldn't start verification of %s.", email)
    return verified_emails


def verify_domains(domain_list, ses_client):
    """
    Starts verification for a list of domain identities. This returns a token for
    each domain, which must be registered as a TXT record with the DNS provider
 for
    the domain.

    :param domain_list: The list of domains to verify.
    :param ses_client: A Boto3 Amazon SES client.
    :return: The generated domain tokens to use to completed verification.
    """
    domain_tokens = {}
    for domain in domain_list:
        try:
            response = ses_client.verify_domain_identity(Domain=domain)
            token = response["VerificationToken"]
            domain_tokens[domain] = token
            logger.info("Got verification token %s for domain %s.", token,
 domain)
        except ClientError:
            logger.warning("Couldn't get verification token for domain %s.",
 domain)
```

```
    return domain_tokens


def get_hosted_zones(route53_client):
    """
    Gets the Amazon Route 53 hosted zones for the current account.

    :param route53_client: A Boto3 Route 53 client.
    :return: The list of hosted zones.
    """
    zones = []
    try:
        zone_paginator = route53_client.get_paginator("list_hosted_zones")
        zone_iterator = zone_paginator.paginate(PaginationConfig={"PageSize":
 20})
        zones = [
            zone for zone_page in zone_iterator for zone in
 zone_page["HostedZones"]
        ]
        logger.info("Found %s hosted zones.", len(zones))
    except ClientError:
        logger.warning("Couldn't get hosted zones.")
    return zones


def find_domain_zone_matches(domains, zones):
    """
    Finds matches between Amazon SES verified domains and Route 53 hosted zones.
    Subdomain matches are taken when found, otherwise root domain matches are
 taken.

    :param domains: The list of domains to match.
    :param zones: The list of hosted zones to match.
    :return: The set of matched domain-zone pairs. When a match is not found, the
             domain is included in the set with a zone value of None.
    """
    domain_zones = {}
    for domain in domains:
        domain_zones[domain] = None
        # Start at the most specific sub-domain and walk up to the root domain
 until a
        # zone match is found.
        domain_split = domain.split(".")
        for index in range(0, len(domain_split) - 1):
```

```
            sub_domain = ".".join(domain_split[index:])
            for zone in zones:
                # Normalize the zone name from Route 53 by removing the trailing
 '.'.
                zone_name = zone["Name"][:-1]
                if sub_domain == zone_name:
                    domain_zones[domain] = zone
                    break
            if domain_zones[domain] is not None:
                break
    return domain_zones


def add_route53_verification_record(domain, token, zone, route53_client):
    """
    Adds a domain verification TXT record to the specified Route 53 hosted zone.
    When a TXT record already exists in the hosted zone for the specified domain,
    the existing values are preserved and the new token is added to the list.

    :param domain: The domain to add.
    :param token: The verification token for the domain.
    :param zone: The hosted zone where the domain verification record is added.
    :param route53_client: A Boto3 Route 53 client.
    """
    domain_token_record_set_name = f"_amazonses.{domain}"
    record_set_paginator =
 route53_client.get_paginator("list_resource_record_sets")
    record_set_iterator = record_set_paginator.paginate(
        HostedZoneId=zone["Id"], PaginationConfig={"PageSize": 20}
    )
    records = []
    for record_set_page in record_set_iterator:
        try:
            txt_record_set = next(
                record_set
                for record_set in record_set_page["ResourceRecordSets"]
                if record_set["Name"][:-1] == domain_token_record_set_name
                and record_set["Type"] == "TXT"
            )
            records = txt_record_set["ResourceRecords"]
            logger.info(
                "Existing TXT record found in set %s for zone %s.",
                domain_token_record_set_name,
                zone["Name"],
```

```
            )
            break
        except StopIteration:
            pass
    records.append({"Value": json.dumps(token)})
    changes = [
        {
            "Action": "UPSERT",
            "ResourceRecordSet": {
                "Name": domain_token_record_set_name,
                "Type": "TXT",
                "TTL": 1800,
                "ResourceRecords": records,
            },
        }
    ]
    try:
        route53_client.change_resource_record_sets(
            HostedZoneId=zone["Id"], ChangeBatch={"Changes": changes}
        )
        logger.info(
            "Created or updated the TXT record in set %s for zone %s.",
            domain_token_record_set_name,
            zone["Name"],
        )
    except ClientError as err:
        logger.warning(
            "Got error %s. Couldn't create or update the TXT record for zone
 %s.",
            err.response["Error"]["Code"],
            zone["Name"],
        )


def generate_dkim_tokens(domain, ses_client):
    """
    Generates DKIM tokens for a domain. These must be added as CNAME records to
 the
    DNS provider for the domain.

    :param domain: The domain to generate tokens for.
    :param ses_client: A Boto3 Amazon SES client.
    :return: The list of generated DKIM tokens.
    """
```

```
    dkim_tokens = []
    try:
        dkim_tokens = ses_client.verify_domain_dkim(Domain=domain)["DkimTokens"]
        logger.info("Generated %s DKIM tokens for domain %s.", len(dkim_tokens),
 domain)
    except ClientError:
        logger.warning("Couldn't generate DKIM tokens for domain %s.", domain)
    return dkim_tokens


def add_dkim_domain_tokens(hosted_zone, domain, tokens, route53_client):
    """
    Adds DKIM domain token CNAME records to a Route 53 hosted zone.

    :param hosted_zone: The hosted zone where the records are added.
    :param domain: The domain to add.
    :param tokens: The DKIM tokens for the domain to add.
    :param route53_client: A Boto3 Route 53 client.
    """
    try:
        changes = [
            {
                "Action": "UPSERT",
                "ResourceRecordSet": {
                    "Name": f"{token}._domainkey.{domain}",
                    "Type": "CNAME",
                    "TTL": 1800,
                    "ResourceRecords": [{"Value":
 f"{token}.dkim.amazonses.com"}],
                },
            }
            for token in tokens
        ]
        route53_client.change_resource_record_sets(
            HostedZoneId=hosted_zone["Id"], ChangeBatch={"Changes": changes}
        )
        logger.info(
            "Added %s DKIM CNAME records to %s in zone %s.",
            len(tokens),
            domain,
            hosted_zone["Name"],
        )
    except ClientError:
        logger.warning(
```

```
            "Couldn't add DKIM CNAME records for %s to zone %s.",
            domain,
            hosted_zone["Name"],
        )


def configure_sns_topics(identity, topics, ses_client):
    """
    Configures Amazon Simple Notification Service (Amazon SNS) notifications for
    an identity. The Amazon SNS topics must already exist.

    :param identity: The identity to configure.
    :param topics: The list of topics to configure. The choices are Bounce,
 Delivery,
                   or Complaint.
    :param ses_client: A Boto3 Amazon SES client.
    """
    for topic in topics:
        topic_arn = input(
            f"Enter the Amazon Resource Name (ARN) of the {topic} topic or press
 "
            f"Enter to skip: "
        )
        if topic_arn != "":
            try:
                ses_client.set_identity_notification_topic(
                    Identity=identity, NotificationType=topic, SnsTopic=topic_arn
                )
                logger.info("Configured %s for %s notifications.", identity,
 topic)
            except ClientError:
                logger.warning(
                    "Couldn't configure %s for %s notifications.", identity,
 topic
                )


def replicate(source_client, destination_client, route53_client):
    logging.basicConfig(level=logging.INFO, format="%(levelname)s: %(message)s")

    print("-" * 88)
    print(
        f"Replicating Amazon SES identities and other configuration from "
```

```
        f"{source_client.meta.region_name} to
 {destination_client.meta.region_name}."
    )
    print("-" * 88)

    print(f"Retrieving identities from {source_client.meta.region_name}.")
    source_emails, source_domains = get_identities(source_client)
    print("Email addresses found:")
    print(*source_emails)
    print("Domains found:")
    print(*source_domains)

    print("Starting verification for email identities.")
    dest_emails = verify_emails(source_emails, destination_client)
    print("Getting domain tokens for domain identities.")
    dest_domain_tokens = verify_domains(source_domains, destination_client)

    # Get Route 53 hosted zones and match them with Amazon SES domains.
    answer = input(
        "Is the DNS configuration for your domains managed by Amazon Route 53 (y/
n)? "
    )
    use_route53 = answer.lower() == "y"
    hosted_zones = get_hosted_zones(route53_client) if use_route53 else []
    if use_route53:
        print("Adding or updating Route 53 TXT records for your domains.")
        domain_zones = find_domain_zone_matches(dest_domain_tokens.keys(),
 hosted_zones)
        for domain in domain_zones:
            add_route53_verification_record(
                domain, dest_domain_tokens[domain], domain_zones[domain],
 route53_client
            )
    else:
        print(
            "Use these verification tokens to create TXT records through your DNS
 "
            "provider:"
        )
        pprint(dest_domain_tokens)

    answer = input("Do you want to configure DKIM signing for your identities (y/
n)? ")
    if answer.lower() == "y":
```

```
        # Build a set of unique domains from email and domain identities.
        domains = {email.split("@")[1] for email in dest_emails}
        domains.update(dest_domain_tokens)
        domain_zones = find_domain_zone_matches(domains, hosted_zones)
        for domain, zone in domain_zones.items():
            answer = input(
                f"Do you want to configure DKIM signing for {domain} (y/n)? "
            )
            if answer.lower() == "y":
                dkim_tokens = generate_dkim_tokens(domain, destination_client)
                if use_route53 and zone is not None:
                    add_dkim_domain_tokens(zone, domain, dkim_tokens,
 route53_client)
                else:
                    print(
                        "Add the following DKIM tokens as CNAME records through
 your "
                        "DNS provider:"
                    )
                    print(*dkim_tokens, sep="\n")

    answer = input(
        "Do you want to configure Amazon SNS notifications for your identities
 (y/n)? "
    )
    if answer.lower() == "y":
        for identity in dest_emails + list(dest_domain_tokens.keys()):
            answer = input(
                f"Do you want to configure Amazon SNS topics for {identity} (y/
n)? "
            )
            if answer.lower() == "y":
                configure_sns_topics(
                    identity, ["Bounce", "Delivery", "Complaint"],
 destination_client
                )

    print(f"Replication complete for {destination_client.meta.region_name}.")
    print("-" * 88)


def main():
    boto3_session = boto3.Session()
    ses_regions = boto3_session.get_available_regions("ses")
```

```
    parser = argparse.ArgumentParser(
        description="Copies email address and domain identities from one AWS
 Region to "
        "another. Optionally adds records for domain verification and DKIM "
        "signing to domains that are managed by Amazon Route 53, "
        "and sets up Amazon SNS notifications for events of interest."
    )
    parser.add_argument(
        "source_region", choices=ses_regions, help="The region to copy from."
    )
    parser.add_argument(
        "destination_region", choices=ses_regions, help="The region to copy to."
    )
    args = parser.parse_args()
    source_client = boto3.client("ses", region_name=args.source_region)
    destination_client = boto3.client("ses", region_name=args.destination_region)
    route53_client = boto3.client("route53")
    replicate(source_client, destination_client, route53_client)


if __name__ == "__main__":
    main()
```

- Pour plus d'informations sur l'API, consultez les rubriques suivantes dans AWS SDK for Python (Boto3) API Reference.
  - ListIdentities
  - SetIdentityNotificationTopic
  - VerifyDomainDkim
  - VerifyDomainIdentity
  - VerifyEmailIdentity

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Générer des informations d'identification pour vous connecter à un point de terminaison d'un SMTP Amazon SES

L'exemple de code suivant montre comment générer des informations d'identification pour vous connecter à un point de terminaison d'un SMTP Amazon SES.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
#!/usr/bin/env python3

import hmac
import hashlib
import base64
import argparse

SMTP_REGIONS = [
    "us-east-2",  # US East (Ohio)
    "us-east-1",  # US East (N. Virginia)
    "us-west-2",  # US West (Oregon)
    "ap-south-1",  # Asia Pacific (Mumbai)
    "ap-northeast-2",  # Asia Pacific (Seoul)
    "ap-southeast-1",  # Asia Pacific (Singapore)
    "ap-southeast-2",  # Asia Pacific (Sydney)
    "ap-northeast-1",  # Asia Pacific (Tokyo)
    "ca-central-1",  # Canada (Central)
    "eu-central-1",  # Europe (Frankfurt)
    "eu-west-1",  # Europe (Ireland)
    "eu-west-2",  # Europe (London)
    "eu-south-1",  # Europe (Milan)
    "eu-north-1",  # Europe (Stockholm)
    "sa-east-1",  # South America (Sao Paulo)
    "us-gov-west-1",  # AWS GovCloud (US)
]
```

```
# These values are required to calculate the signature. Do not change them.
DATE = "11111111"
SERVICE = "ses"
MESSAGE = "SendRawEmail"
TERMINAL = "aws4_request"
VERSION = 0x04


def sign(key, msg):
    return hmac.new(key, msg.encode("utf-8"), hashlib.sha256).digest()


def calculate_key(secret_access_key, region):
    if region not in SMTP_REGIONS:
        raise ValueError(f"The {region} Region doesn't have an SMTP endpoint.")

    signature = sign(("AWS4" + secret_access_key).encode("utf-8"), DATE)
    signature = sign(signature, region)
    signature = sign(signature, SERVICE)
    signature = sign(signature, TERMINAL)
    signature = sign(signature, MESSAGE)
    signature_and_version = bytes([VERSION]) + signature
    smtp_password = base64.b64encode(signature_and_version)
    return smtp_password.decode("utf-8")


def main():
    parser = argparse.ArgumentParser(
        description="Convert a Secret Access Key to an SMTP password."
    )
    parser.add_argument("secret", help="The Secret Access Key to convert.")
    parser.add_argument(
        "region",
        help="The AWS Region where the SMTP password will be used.",
        choices=SMTP_REGIONS,
    )
    args = parser.parse_args()
    print(calculate_key(args.secret, args.region))


if __name__ == "__main__":
    main()
```

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Vérifiez une identité e-mail et envoyez des messages avec Amazon SES à l'aide d'un AWS SDK

L'exemple de code suivant illustre comment :

- Ajoutez et vérifiez une adresse e-mail avec Amazon SES.
- Envoyez un e-mail standard.
- Créez un modèle et envoyez un e-mail basé sur un modèle.
- Envoyez un message en utilisant un serveur SMTP Amazon SES.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Vérifiez une adresse e-mail avec Amazon SES et envoyez des messages.

```
def usage_demo():
    print("-" * 88)
    print("Welcome to the Amazon Simple Email Service (Amazon SES) email demo!")
    print("-" * 88)

    logging.basicConfig(level=logging.INFO, format="%(levelname)s: %(message)s")

    ses_client = boto3.client("ses")
    ses_identity = SesIdentity(ses_client)
    ses_mail_sender = SesMailSender(ses_client)
    ses_template = SesTemplate(ses_client)
    email = input("Enter an email address to send mail with Amazon SES: ")
    status = ses_identity.get_identity_status(email)
    verified = status == "Success"
```

```
    if not verified:
        answer = input(
            f"The address '{email}' is not verified with Amazon SES. Unless your
"
            f"Amazon SES account is out of sandbox, you can send mail only from "
            f"and to verified accounts. Do you want to verify this account for
use "
            f"with Amazon SES? If yes, the address will receive a verification "
            f"email (y/n): "
        )
        if answer.lower() == "y":
            ses_identity.verify_email_identity(email)
            print(f"Follow the steps in the email to {email} to complete
verification.")
            print("Waiting for verification...")
            try:
                ses_identity.wait_until_identity_exists(email)
                print(f"Identity verified for {email}.")
                verified = True
            except WaiterError:
                print(
                    f"Verification timeout exceeded. You must complete the "
                    f"steps in the email sent to {email} to verify the address."
                )

    if verified:
        test_message_text = "Hello from the Amazon SES mail demo!"
        test_message_html = "<p>Hello!</p><p>From the <b>Amazon SES</b> mail
demo!</p>"

        print(f"Sending mail from {email} to {email}.")
        ses_mail_sender.send_email(
            email,
            SesDestination([email]),
            "Amazon SES demo",
            test_message_text,
            test_message_html,
        )
        input("Mail sent. Check your inbox and press Enter to continue.")

        template = {
            "name": "doc-example-template",
            "subject": "Example of an email template.",
```

```
            "text": "This is what {{name}} will {{action}} if {{name}} can't
 display "
            "HTML.",
            "html": "<p><i>This</i> is what {{name}} will {{action}} if {{name}}
 "
            "<b>can</b> display HTML.</p>",
        }
        print("Creating a template and sending a templated email.")
        ses_template.create_template(**template)
        template_data = {"name": email.split("@")[0], "action": "read"}
        if ses_template.verify_tags(template_data):
            ses_mail_sender.send_templated_email(
                email, SesDestination([email]), ses_template.name(),
 template_data
            )
            input("Mail sent. Check your inbox and press Enter to continue.")

        print("Sending mail through the Amazon SES SMTP server.")
        boto3_session = boto3.Session()
        region = boto3_session.region_name
        credentials = boto3_session.get_credentials()
        port = 587
        smtp_server = f"email-smtp.{region}.amazonaws.com"
        password = calculate_key(credentials.secret_key, region)
        message = """
Subject: Hi there

This message is sent from the Amazon SES SMTP mail demo."""
        context = ssl.create_default_context()
        with smtplib.SMTP(smtp_server, port) as server:
            server.starttls(context=context)
            server.login(credentials.access_key, password)
            server.sendmail(email, email, message)
        print("Mail sent. Check your inbox!")

    if ses_template.template is not None:
        print("Deleting demo template.")
        ses_template.delete_template()
    if verified:
        answer = input(f"Do you want to remove {email} from Amazon SES (y/n)? ")
        if answer.lower() == "y":
            ses_identity.delete_identity(email)
    print("Thanks for watching!")
    print("-" * 88)
```

Créer des fonctions pour encapsuler les actions d'identité Amazon SES.

```
class SesIdentity:
    """Encapsulates Amazon SES identity functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client


    def verify_domain_identity(self, domain_name):
        """
        Starts verification of a domain identity. To complete verification, you
 must
        create a TXT record with a specific format through your DNS provider.

        For more information, see *Verifying a domain with Amazon SES* in the
        Amazon SES documentation:
            https://docs.aws.amazon.com/ses/latest/DeveloperGuide/verify-domain-
procedure.html

        :param domain_name: The name of the domain to verify.
        :return: The token to include in the TXT record with your DNS provider.
        """
        try:
            response = self.ses_client.verify_domain_identity(Domain=domain_name)
            token = response["VerificationToken"]
            logger.info("Got domain verification token for %s.", domain_name)
        except ClientError:
            logger.exception("Couldn't verify domain %s.", domain_name)
            raise
        else:
            return token


    def verify_email_identity(self, email_address):
        """
```

```
        Starts verification of an email identity. This function causes an email
        to be sent to the specified email address from Amazon SES. To complete
        verification, follow the instructions in the email.

        :param email_address: The email address to verify.
        """
        try:
            self.ses_client.verify_email_identity(EmailAddress=email_address)
            logger.info("Started verification of %s.", email_address)
        except ClientError:
            logger.exception("Couldn't start verification of %s.", email_address)
            raise


    def wait_until_identity_exists(self, identity):
        """
        Waits until an identity exists. The waiter polls Amazon SES until the
        identity has been successfully verified or until it exceeds its maximum
time.

        :param identity: The identity to wait for.
        """
        try:
            waiter = self.ses_client.get_waiter("identity_exists")
            logger.info("Waiting until %s exists.", identity)
            waiter.wait(Identities=[identity])
        except WaiterError:
            logger.error("Waiting for identity %s failed or timed out.",
identity)
            raise


    def get_identity_status(self, identity):
        """
        Gets the status of an identity. This can be used to discover whether
        an identity has been successfully verified.

        :param identity: The identity to query.
        :return: The status of the identity.
        """
        try:
            response = self.ses_client.get_identity_verification_attributes(
                Identities=[identity]
            )
```

```
            status = response["VerificationAttributes"].get(
                identity, {"VerificationStatus": "NotFound"}
            )["VerificationStatus"]
            logger.info("Got status of %s for %s.", status, identity)
        except ClientError:
            logger.exception("Couldn't get status for %s.", identity)
            raise
        else:
            return status


    def delete_identity(self, identity):
        """
        Deletes an identity.

        :param identity: The identity to remove.
        """
        try:
            self.ses_client.delete_identity(Identity=identity)
            logger.info("Deleted identity %s.", identity)
        except ClientError:
            logger.exception("Couldn't delete identity %s.", identity)
            raise


    def list_identities(self, identity_type, max_items):
        """
        Gets the identities of the specified type for the current account.

        :param identity_type: The type of identity to retrieve, such as
EmailAddress.
        :param max_items: The maximum number of identities to retrieve.
        :return: The list of retrieved identities.
        """
        try:
            response = self.ses_client.list_identities(
                IdentityType=identity_type, MaxItems=max_items
            )
            identities = response["Identities"]
            logger.info("Got %s identities for the current account.",
len(identities))
        except ClientError:
            logger.exception("Couldn't list identities for the current account.")
            raise
```

```
        else:
            return identities
```

Créer des fonctions pour encapsuler les actions de modèle Amazon SES.

```
class SesTemplate:
    """Encapsulates Amazon SES template functions."""

    def __init__(self, ses_client):
        """
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client
        self.template = None
        self.template_tags = set()

    def _extract_tags(self, subject, text, html):
        """
        Extracts tags from a template as a set of unique values.

        :param subject: The subject of the email.
        :param text: The text version of the email.
        :param html: The html version of the email.
        """
        self.template_tags = set(re.findall(TEMPLATE_REGEX, subject + text +
 html))
        logger.info("Extracted template tags: %s", self.template_tags)


    def create_template(self, name, subject, text, html):
        """
        Creates an email template.

        :param name: The name of the template.
        :param subject: The subject of the email.
        :param text: The plain text version of the email.
        :param html: The HTML version of the email.
        """
        try:
            template = {
```

```
                "TemplateName": name,
                "SubjectPart": subject,
                "TextPart": text,
                "HtmlPart": html,
            }
            self.ses_client.create_template(Template=template)
            logger.info("Created template %s.", name)
            self.template = template
            self._extract_tags(subject, text, html)
        except ClientError:
            logger.exception("Couldn't create template %s.", name)
            raise


    def delete_template(self):
        """
        Deletes an email template.
        """
        try:

self.ses_client.delete_template(TemplateName=self.template["TemplateName"])
            logger.info("Deleted template %s.", self.template["TemplateName"])
            self.template = None
            self.template_tags = None
        except ClientError:
            logger.exception(
                "Couldn't delete template %s.", self.template["TemplateName"]
            )
            raise


    def get_template(self, name):
        """
        Gets a previously created email template.

        :param name: The name of the template to retrieve.
        :return: The retrieved email template.
        """
        try:
            response = self.ses_client.get_template(TemplateName=name)
            self.template = response["Template"]
            logger.info("Got template %s.", name)
            self._extract_tags(
                self.template["SubjectPart"],
```

```
                self.template["TextPart"],
                self.template["HtmlPart"],
            )
        except ClientError:
            logger.exception("Couldn't get template %s.", name)
            raise
        else:
            return self.template


    def list_templates(self):
        """
        Gets a list of all email templates for the current account.

        :return: The list of retrieved email templates.
        """
        try:
            response = self.ses_client.list_templates()
            templates = response["TemplatesMetadata"]
            logger.info("Got %s templates.", len(templates))
        except ClientError:
            logger.exception("Couldn't get templates.")
            raise
        else:
            return templates


    def update_template(self, name, subject, text, html):
        """
        Updates a previously created email template.

        :param name: The name of the template.
        :param subject: The subject of the email.
        :param text: The plain text version of the email.
        :param html: The HTML version of the email.
        """
        try:
            template = {
                "TemplateName": name,
                "SubjectPart": subject,
                "TextPart": text,
                "HtmlPart": html,
            }
            self.ses_client.update_template(Template=template)
```

```
            logger.info("Updated template %s.", name)
            self.template = template
            self._extract_tags(subject, text, html)
        except ClientError:
            logger.exception("Couldn't update template %s.", name)
            raise
```

Créer des fonctions pour encapsuler les actions e-mail Amazon SES.

```
class SesDestination:
    """Contains data about an email destination."""

    def __init__(self, tos, ccs=None, bccs=None):
        """
        :param tos: The list of recipients on the 'To:' line.
        :param ccs: The list of recipients on the 'CC:' line.
        :param bccs: The list of recipients on the 'BCC:' line.
        """
        self.tos = tos
        self.ccs = ccs
        self.bccs = bccs

    def to_service_format(self):
        """
        :return: The destination data in the format expected by Amazon SES.
        """
        svc_format = {"ToAddresses": self.tos}
        if self.ccs is not None:
            svc_format["CcAddresses"] = self.ccs
        if self.bccs is not None:
            svc_format["BccAddresses"] = self.bccs
        return svc_format



class SesMailSender:
    """Encapsulates functions to send emails with Amazon SES."""

    def __init__(self, ses_client):
        """
```

```
        :param ses_client: A Boto3 Amazon SES client.
        """
        self.ses_client = ses_client


    def send_email(self, source, destination, subject, text, html,
reply_tos=None):
        """
        Sends an email.

        Note: If your account is in the Amazon SES  sandbox, the source and
        destination email accounts must both be verified.

        :param source: The source email account.
        :param destination: The destination email account.
        :param subject: The subject of the email.
        :param text: The plain text version of the body of the email.
        :param html: The HTML version of the body of the email.
        :param reply_tos: Email accounts that will receive a reply if the
recipient
                          replies to the message.
        :return: The ID of the message, assigned by Amazon SES.
        """
        send_args = {
            "Source": source,
            "Destination": destination.to_service_format(),
            "Message": {
                "Subject": {"Data": subject},
                "Body": {"Text": {"Data": text}, "Html": {"Data": html}},
            },
        }
        if reply_tos is not None:
            send_args["ReplyToAddresses"] = reply_tos
        try:
            response = self.ses_client.send_email(**send_args)
            message_id = response["MessageId"]
            logger.info(
                "Sent mail %s from %s to %s.", message_id, source,
destination.tos
            )
        except ClientError:
            logger.exception(
                "Couldn't send mail from %s to %s.", source, destination.tos
            )
```

```
            raise
        else:
            return message_id


    def send_templated_email(
        self, source, destination, template_name, template_data, reply_tos=None
    ):
        """
        Sends an email based on a template. A template contains replaceable tags
        each enclosed in two curly braces, such as {{name}}. The template data
passed
        in this function contains key-value pairs that define the values to
insert
        in place of the template tags.

        Note: If your account is in the Amazon SES  sandbox, the source and
        destination email accounts must both be verified.

        :param source: The source email account.
        :param destination: The destination email account.
        :param template_name: The name of a previously created template.
        :param template_data: JSON-formatted key-value pairs of replacement
values
                              that are inserted in the template before it is
sent.
        :return: The ID of the message, assigned by Amazon SES.
        """
        send_args = {
            "Source": source,
            "Destination": destination.to_service_format(),
            "Template": template_name,
            "TemplateData": json.dumps(template_data),
        }
        if reply_tos is not None:
            send_args["ReplyToAddresses"] = reply_tos
        try:
            response = self.ses_client.send_templated_email(**send_args)
            message_id = response["MessageId"]
            logger.info(
                "Sent templated mail %s from %s to %s.",
                message_id,
                source,
                destination.tos,
```

```
            )
        except ClientError:
            logger.exception(
                "Couldn't send templated mail from %s to %s.", source,
destination.tos
            )
            raise
        else:
            return message_id
```

- Pour plus d'informations sur l'API, consultez les rubriques suivantes dans AWS SDK for Python (Boto3) API Reference.
  - CreateTemplate
  - DeleteIdentity
  - DeleteTemplate
  - GetIdentityVerificationAttributes
  - GetTemplate
  - ListIdentities
  - ListTemplates
  - SendEmail
  - SendTemplatedEmail
  - UpdateTemplate
  - VerifyDomainIdentity
  - VerifyEmailIdentity

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Exemples multiservices pour Amazon SES utilisant AWS des kits de développement logiciel

Les exemples d'applications suivants utilisent des AWS SDK pour associer Amazon SES à d'autres Services AWS applications. Chaque exemple inclut un lien vers GitHub, où vous pouvez trouver des instructions sur la façon de configurer et d'exécuter l'application.

Exemples

- Créer une application de streaming Amazon Transcribe
- Créer une application web pour suivre les données DynamoDB
- Créer un outil de suivi des éléments Amazon Redshift.
- Créer un outil de suivi des éléments de travail sans serveur Aurora
- Détectez le PPE dans les images avec Amazon Rekognition à l'aide d'un SDK AWS
- Détectez des objets dans des images avec Amazon Rekognition à l'aide d'un SDK AWS
- Détectez les personnes et les objets dans une vidéo avec Amazon Rekognition à l'aide d'un SDK AWS
- Utiliser les fonctions Step Functions pour invoquer des fonctions Lambda

Créer une application de streaming Amazon Transcribe

L’exemple de code suivant montre comment créer une application qui enregistre, transcrit et traduit de l’audio en direct en temps réel, et envoie les résultats par e-mail.

JavaScript

SDK pour JavaScript (v3)

Montre comment utiliser Amazon Transcribe afin de créer une application qui enregistre, transcrit et traduit de l’audio en direct en temps réel, et envoie les résultats par e-mail à l’aide d’Amazon Simple Email Service (Amazon SES).

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- Amazon Comprehend

- Amazon SES
- Amazon Transcribe
- Amazon Translate

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Créer une application web pour suivre les données DynamoDB

Les exemples de code suivants montrent comment créer une application web qui suit des éléments de travail dans une table Amazon DynamoDB et envoie des rapports par e-mail à l'aide d'Amazon Simple Email Service (Amazon SES).

.NET

AWS SDK for .NET

Montre comment utiliser l'API Amazon DynamoDB .NET pour créer une application web dynamique qui suit les données de travail DynamoDB.

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- DynamoDB
- Amazon SES

Java

SDK pour Java 2.x

Montre comment utiliser l'API Amazon DynamoDB pour créer une application web dynamique qui suit les données de travail DynamoDB.

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- DynamoDB
- Amazon SES

JavaScript

SDK pour JavaScript (v3)

Montre comment utiliser l'API Amazon DynamoDB pour créer une application web dynamique qui suit les données de travail DynamoDB.

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- DynamoDB
- Amazon SES

Kotlin

SDK pour Kotlin

Montre comment utiliser l'API Amazon DynamoDB pour créer une application web dynamique qui suit les données de travail DynamoDB.

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- DynamoDB
- Amazon SES

Python

SDK pour Python (Boto3)

Montre comment utiliser le AWS SDK for Python (Boto3) pour créer un service REST qui suit les éléments de travail dans Amazon DynamoDB et envoie des rapports par e-mail à l'aide

d'Amazon Simple Email Service (Amazon SES). Cet exemple utilise la structure web Flask pour gérer le routage HTTP et s'intègre à une page web React pour présenter une application web entièrement fonctionnelle.

- Créez un service Flask REST qui s'intègre à Services AWS.
- Lisez, écrivez et mettez à jour les éléments de travail stockés dans une table DynamoDB.
- Utilisez Amazon SES pour envoyer des rapports par e-mail sur les éléments de travail.

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet dans le référentiel d'exemples de AWS code sur GitHub.

Les services utilisés dans cet exemple

- DynamoDB
- Amazon SES

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Créer un outil de suivi des éléments Amazon Redshift.

Les exemples de code suivants montrent comment créer une application web qui suit et crée des rapports sur les éléments de travail à l'aide d'une base de données Amazon Redshift.

Java

SDK pour Java 2.x

Montre comment créer une application web qui suit et génère des rapports sur les éléments de travail stockés dans une base de données Amazon Redshift.

Pour obtenir le code source complet et les instructions sur la façon de configurer une API Spring REST qui interroge les données Amazon Redshift et pour une utilisation par une application React, consultez l'exemple complet sur. GitHub

Les services utilisés dans cet exemple

- Amazon Redshift
- Amazon SES

Kotlin

SDK pour Kotlin

Montre comment créer une application web qui suit et génère des rapports sur les éléments de travail stockés dans une base de données Amazon Redshift.

Pour obtenir le code source complet et les instructions sur la façon de configurer une API Spring REST qui interroge les données Amazon Redshift et pour une utilisation par une application React, consultez l'exemple complet sur. GitHub

Les services utilisés dans cet exemple

- Amazon Redshift
- Amazon SES

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Créer un outil de suivi des éléments de travail sans serveur Aurora

Les exemples de code suivants montrent comment créer une application web qui suit des éléments de travail dans une base de données Amazon Aurora sans serveur et envoie des rapports par e-mail à l'aide d'Amazon Simple Email Service (Amazon SES).

.NET

AWS SDK for .NET

Montre comment utiliser le AWS SDK for .NET pour créer une application Web qui suit les éléments de travail dans une base de données Amazon Aurora et envoie des rapports par e-mail à l'aide d'Amazon Simple Email Service (Amazon SES). Cet exemple utilise un front end créé avec React.js pour interagir avec un backend RESTful .NET.

- Intégrez une application Web React à AWS des services.
- Listez, ajoutez et mettez à jour des éléments dans une table Aurora.
- Envoyez un rapport par e-mail sur les éléments de travail filtrés à l'aide d'Amazon SES.
- Déployez et gérez des exemples de ressources à l'aide du AWS CloudFormation script inclus.

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- Aurora
- Amazon RDS
- Services de données Amazon RDS
- Amazon SES

C++

SDK pour C++

Montre comment créer une application web qui suit et génère des rapports sur les éléments de travail stockés dans une base de données Amazon Aurora sans serveur.

Pour obtenir le code source complet et les instructions sur la façon de configurer une API REST C++ qui interroge les données Amazon Aurora Serverless et à utiliser par une application React, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- Aurora
- Amazon RDS
- Services de données Amazon RDS
- Amazon SES

Java

SDK pour Java 2.x

Montre comment créer une application web qui suit et génère des rapports sur les éléments de travail stockés dans une base de données Amazon RDS.

Pour obtenir le code source complet et les instructions sur la façon de configurer une API Spring REST qui interroge les données Amazon Aurora Serverless et pour une utilisation par une application React, consultez l'exemple complet sur GitHub.

Pour obtenir le code source complet et les instructions sur la façon de configurer et d'exécuter un exemple utilisant l'API JDBC, consultez l'exemple complet sur. GitHub

Les services utilisés dans cet exemple

- Aurora
- Amazon RDS
- Services de données Amazon RDS
- Amazon SES

JavaScript

SDK pour JavaScript (v3)

Montre comment utiliser le AWS SDK for JavaScript (v3) pour créer une application Web qui suit les éléments de travail dans une base de données Amazon Aurora et envoie des rapports par e-mail à l'aide d'Amazon Simple Email Service (Amazon SES). Cet exemple utilise un front end créé avec React.js pour interagir avec un backend Express Node.js.

- Intégrez une application Web React.js à Services AWS.
- Lister, ajouter et mettre à jour des éléments dans une table Aurora.
- Envoyez un rapport par e-mail sur les éléments de travail filtrés en utilisant Amazon SES.
- Déployez et gérez des exemples de ressources à l'aide du AWS CloudFormation script inclus.

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- Aurora
- Amazon RDS
- Services de données Amazon RDS
- Amazon SES

Kotlin

SDK pour Kotlin

Montre comment créer une application web qui suit et génère des rapports sur les éléments de travail stockés dans une base de données Amazon RDS.

Pour obtenir le code source complet et les instructions sur la façon de configurer une API Spring REST qui interroge les données Amazon Aurora Serverless et pour une utilisation par une application React, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- Aurora
- Amazon RDS
- Services de données Amazon RDS
- Amazon SES

PHP

Kit SDK pour PHP

Montre comment utiliser le AWS SDK for PHP pour créer une application Web qui suit les éléments de travail dans une base de données Amazon RDS et envoie des rapports par e-mail à l'aide d'Amazon Simple Email Service (Amazon SES). Cet exemple utilise un frontend créé avec React.js pour interagir avec un backend PHP RESTful.

- Intégrez une application Web React.js à AWS des services.
- Répertoriez, ajoutez, mettez à jour et supprimez des éléments dans une table Amazon RDS.
- Envoyez un rapport par e-mail sur les éléments de travail filtrés à l'aide d'Amazon SES.
- Déployez et gérez des exemples de ressources à l'aide du AWS CloudFormation script inclus.

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- Aurora
- Amazon RDS

- Services de données Amazon RDS
- Amazon SES

Python

SDK pour Python (Boto3)

Montre comment utiliser le AWS SDK for Python (Boto3) pour créer un service REST qui suit les éléments de travail dans une base de données Amazon Aurora Serverless et envoie des rapports par e-mail à l'aide d'Amazon Simple Email Service (Amazon SES). Cet exemple utilise la structure web Flask pour gérer le routage HTTP et s'intègre à une page web React pour présenter une application web entièrement fonctionnelle.

- Créez un service Flask REST qui s'intègre à Services AWS.
- Lisez, écrivez et mettez à jour les éléments de travail stockés dans une base de données Aurora sans serveur.
- Créez un AWS Secrets Manager secret contenant les informations d'identification de la base de données et utilisez-le pour authentifier les appels à la base de données.
- Utilisez Amazon SES pour envoyer des rapports par e-mail sur les éléments de travail.

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- Aurora
- Amazon RDS
- Services de données Amazon RDS
- Amazon SES

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Détectez le PPE dans les images avec Amazon Rekognition à l'aide d'un SDK AWS

Les exemples de code suivants montrent comment créer une application qui utilise Amazon Rekognition afin de détecter l'équipement de protection individuelle (EPI) dans les images.

Java

SDK pour Java 2.x

Montre comment créer une AWS Lambda fonction qui détecte les images à l'aide d'un équipement de protection individuelle.

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- DynamoDB
- Amazon Rekognition
- Amazon S3
- Amazon SES

JavaScript

SDK pour JavaScript (v3)

Montre comment utiliser Amazon Rekognition AWS SDK for JavaScript pour créer une application permettant de détecter les équipements de protection individuelle (EPI) sur des images situées dans un compartiment Amazon Simple Storage Service (Amazon S3). L'application enregistre les résultats dans une table Amazon DynamoDB et envoie à l'administrateur une notification par e-mail contenant les résultats à l'aide d'Amazon Simple Email Service (Amazon SES).

Découvrez comment :

- Créer un utilisateur non authentifié à l'aide d'Amazon Cognito.
- Analyser les images à la recherche d'EPI à l'aide d'Amazon Rekognition.
- Vérifier une adresse e-mail pour Amazon SES.
- Mettre à jour une table DynamoDB avec les résultats.
- Envoyer une notification par e-mail à l'aide d'Amazon SES.

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- DynamoDB
- Amazon Rekognition
- Amazon S3
- Amazon SES

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Détectez des objets dans des images avec Amazon Rekognition à l'aide d'un SDK AWS

Les exemples de code suivants montrent comment créer une application qui utilise Amazon Rekognition afin de détecter des objets par catégorie dans des images.

.NET

AWS SDK for .NET

Montre comment utiliser l'API Java Amazon Rekognition afin de créer une application qui, avec Amazon Rekognition, permet d'identifier des objets par catégorie dans des images stockées dans un compartiment Amazon Simple Storage Service (Amazon S3). L'application envoie à l'administrateur une notification par e-mail contenant les résultats à l'aide d'Amazon Simple Email Service (Amazon SES).

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- Amazon Rekognition
- Amazon S3
- Amazon SES

Java

SDK pour Java 2.x

Montre comment utiliser l'API Java Amazon Rekognition afin de créer une application qui, avec Amazon Rekognition, permet d'identifier des objets par catégorie dans des images stockées dans un compartiment Amazon Simple Storage Service (Amazon S3). L'application envoie à l'administrateur une notification par e-mail contenant les résultats à l'aide d'Amazon Simple Email Service (Amazon SES).

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- Amazon Rekognition
- Amazon S3
- Amazon SES

JavaScript

SDK pour JavaScript (v3)

Montre comment utiliser Amazon Rekognition AWS SDK for JavaScript pour créer une application qui utilise Amazon Rekognition pour identifier les objets par catégorie dans des images situées dans un compartiment Amazon Simple Storage Service (Amazon S3). L'application envoie à l'administrateur une notification par e-mail contenant les résultats à l'aide d'Amazon Simple Email Service (Amazon SES).

Découvrez comment :

- Créer un utilisateur non authentifié à l'aide d'Amazon Cognito.
- Analyser les images à la recherche d'objets à l'aide d'Amazon Rekognition.
- Vérifier une adresse e-mail pour Amazon SES.
- Envoyer une notification par e-mail à l'aide d'Amazon SES.

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- Amazon Rekognition
- Amazon S3
- Amazon SES

Kotlin

SDK pour Kotlin

Montre comment utiliser l'API Kotlin Amazon Rekognition afin de créer une application qui, avec Amazon Rekognition, permet d'identifier des objets par catégorie dans des images stockées dans un compartiment Amazon Simple Storage Service (Amazon S3). L'application envoie à l'administrateur une notification par e-mail contenant les résultats à l'aide d'Amazon Simple Email Service (Amazon SES).

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- Amazon Rekognition
- Amazon S3
- Amazon SES

Python

SDK pour Python (Boto3)

Vous montre comment utiliser le AWS SDK for Python (Boto3) pour créer une application Web qui vous permet d'effectuer les opérations suivantes :

- Chargez les photos dans un compartiment Amazon Simple Storage Service (Amazon S3).
- Utilisez Amazon Rekognition pour analyser et étiqueter les photos.
- Utilisez Amazon Simple Email Service (Amazon SES) pour envoyer des rapports d'analyse d'images par e-mail.

Cet exemple contient deux composants principaux : une page Web écrite avec React et un service REST écrit en Python construit avec Flask-RESTful. JavaScript

Vous pouvez utiliser la page web React pour :

- Affichez une liste d'images stockées dans votre compartiment S3.
- Chargez des images depuis votre ordinateur dans votre compartiment S3.
- Affichez des images et des étiquettes qui identifient les éléments détectés dans l'image.
- Obtenez un rapport de toutes les images de votre compartiment S3 et envoyez un e-mail du rapport.

La page web appelle le service REST. Le service envoie des demandes à AWS pour effectuer les opérations suivantes :

- Obtenez et filtrez la liste des images de votre compartiment S3.
- Chargez des photos dans votre compartiment S3.
- Utilisez Amazon Rekognition pour analyser des photos individuelles et obtenir une liste d'étiquettes qui identifient les éléments détectés sur la photo.
- Analysez toutes les photos de votre compartiment S3 et utilisez Amazon SES pour envoyer un rapport par e-mail.

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- Amazon Rekognition
- Amazon S3
- Amazon SES

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Détectez les personnes et les objets dans une vidéo avec Amazon Rekognition à l'aide d'un SDK AWS

Les exemples de code suivants montrent comment détecter des personnes et des objets dans une vidéo avec Amazon Rekognition.

Java

SDK pour Java 2.x

Montre comment utiliser l'API Java Amazon Rekognition afin de créer une application qui détecte les visages et les objets dans des vidéos stockées dans un compartiment Amazon Simple Storage Service (Amazon S3). L'application envoie à l'administrateur une notification par e-mail contenant les résultats à l'aide d'Amazon Simple Email Service (Amazon SES).

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- Amazon Rekognition
- Amazon S3
- Amazon SES

JavaScript

SDK pour JavaScript (v3)

Montre comment utiliser Amazon Rekognition pour créer une application permettant de détecter AWS SDK for JavaScript des visages et des objets dans des vidéos situées dans un compartiment Amazon Simple Storage Service (Amazon S3). L'application envoie à l'administrateur une notification par e-mail contenant les résultats à l'aide d'Amazon Simple Email Service (Amazon SES).

Découvrez comment :

- Créer un utilisateur non authentifié à l'aide d'Amazon Cognito.
- Analyser les images à la recherche d'EPI à l'aide d'Amazon Rekognition.
- Vérifier une adresse e-mail pour Amazon SES.
- Envoyer une notification par e-mail à l'aide d'Amazon SES.

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- Amazon Rekognition

- Amazon S3
- Amazon SES

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utiliser les fonctions Step Functions pour invoquer des fonctions Lambda

Les exemples de code suivants montrent comment créer une machine à AWS Step Functions états qui invoque des AWS Lambda fonctions en séquence.

Java

SDK pour Java 2.x

Montre comment créer un flux de travail AWS sans serveur en utilisant AWS Step Functions et le AWS SDK for Java 2.x. Chaque étape du flux de travail est implémentée à l'aide d'une AWS Lambda fonction.

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Les services utilisés dans cet exemple

- DynamoDB
- Lambda
- Amazon SES
- Step Functions

JavaScript

SDK pour JavaScript (v3)

Montre comment créer un flux de travail AWS sans serveur en utilisant AWS Step Functions et le AWS SDK for JavaScript. Chaque étape du flux de travail est implémentée à l'aide d'une AWS Lambda fonction.

Lambda est un service de calcul qui vous permet d’exécuter du code sans devoir approvisionner ou gérer des serveurs. Step Functions est un service d’orchestration sans

serveur qui vous permet de combiner des fonctions Lambda et d'autres services AWS afin de créer des applications métier essentielles.

Pour obtenir le code source complet et les instructions de configuration et d'exécution, consultez l'exemple complet sur GitHub.

Cet exemple est également disponible dans le AWS SDK for JavaScript guide du développeur v3.

Les services utilisés dans cet exemple

- DynamoDB
- Lambda
- Amazon SES
- Step Functions

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Exemples de code pour l'API Amazon SES v2 à l'aide de AWS kits SDK

Les exemples de code suivants montrent comment utiliser l'API Amazon SES v2 avec un kit de développement AWS logiciel (SDK).

Les actions sont des extraits de code de programmes plus larges et doivent être exécutées dans leur contexte. Alors que les actions vous indiquent comment appeler des fonctions de service individuelles, vous pouvez les voir en contexte dans leurs scénarios associés et dans des exemples interservices.

Les Scénarios sont des exemples de code qui vous montrent comment accomplir une tâche spécifique en appelant plusieurs fonctions au sein d'un même service.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit de développement logiciel (SDK).

Exemples de code

Actions pour l'API Amazon SES v2 à l'aide de AWS kits SDK

Les exemples de code suivants montrent comment effectuer des actions individuelles de l'API Amazon SES v2 avec des AWS SDK. Ces extraits appellent l'API Amazon SES v2 et sont des extraits de code de programmes plus volumineux qui doivent être exécutés en contexte. Chaque exemple inclut un lien vers GitHub, où vous pouvez trouver des instructions pour configurer et exécuter le code.

Les exemples suivants incluent uniquement les actions les plus couramment utilisées. Pour une description complète, veuillez consulter le document Référence de l'API Amazon Simple Email Service.

Exemples

- Utilisation DeleteContactList avec un AWS SDK ou une CLI
- Utilisation DeleteEmailIdentity avec un AWS SDK ou une CLI
- Utilisation DeleteEmailTemplate avec un AWS SDK ou une CLI
- Utilisation GetEmailIdentity avec un AWS SDK ou une CLI
- Utilisation ListContactLists avec un AWS SDK ou une CLI
- Utilisation ListContacts avec un AWS SDK ou une CLI
- Utilisation SendEmail avec un AWS SDK ou une CLI

Utilisation **`CreateContact`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`CreateContact`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Flux de travail des newsletters

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Creates a contact and adds it to the specified contact list.
    /// </summary>
    /// <param name="emailAddress">The email address of the contact.</param>
    /// <param name="contactListName">The name of the contact list.</param>
    /// <returns>The response from the CreateContact operation.</returns>
    public async Task<bool> CreateContactAsync(string emailAddress, string
contactListName)
    {
```

```
        var request = new CreateContactRequest
        {
            EmailAddress = emailAddress,
            ContactListName = contactListName
        };

        try
        {
            var response = await _sesClient.CreateContactAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (AlreadyExistsException ex)
        {
            Console.WriteLine($"Contact with email address {emailAddress} already
exists in the contact list {contactListName}.");
            Console.WriteLine(ex.Message);
            return true;
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The contact list {contactListName} does not
exist.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while creating the contact:
{ex.Message}");
        }
        return false;
    }
```

- Pour plus de détails sur l'API, reportez-vous CreateContactà la section Référence des AWS SDK for .NET API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
      try {
        // Create a new contact with the provided email address in the
        CreateContactRequest contactRequest = CreateContactRequest.builder()
            .contactListName(CONTACT_LIST_NAME)
            .emailAddress(emailAddress)
            .build();

        sesClient.createContact(contactRequest);
        contacts.add(emailAddress);

        System.out.println("Contact created: " + emailAddress);

        // Send a welcome email to the new contact
        String welcomeHtml = Files.readString(Paths.get("resources/
coupon_newsletter/welcome.html"));
        String welcomeText = Files.readString(Paths.get("resources/
coupon_newsletter/welcome.txt"));

        SendEmailRequest welcomeEmailRequest = SendEmailRequest.builder()
            .fromEmailAddress(this.verifiedEmail)
            .destination(Destination.builder().toAddresses(emailAddress).build())
            .content(EmailContent.builder()
                .simple(
                    Message.builder()
                        .subject(Content.builder().data("Welcome to the Weekly
 Coupons Newsletter").build())
                        .body(Body.builder()
                            .text(Content.builder().data(welcomeText).build())
                            .html(Content.builder().data(welcomeHtml).build())
                            .build())
                        .build())
                .build())
```

```
            .build();
        SendEmailResponse welcomeEmailResponse =
sesClient.sendEmail(welcomeEmailRequest);
        System.out.println("Welcome email sent: " +
welcomeEmailResponse.messageId());
     } catch (AlreadyExistsException e) {
        // If the contact already exists, skip this step for that contact and
proceed
        // with the next contact
        System.out.println("Contact already exists, skipping creation...");
     } catch (Exception e) {
        System.err.println("Error occurred while processing email address " +
emailAddress + ": " + e.getMessage());
        throw e;
     }
   }
```

- Pour plus de détails sur l'API, reportez-vous CreateContactà la section Référence des AWS SDK for Java 2.x API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
```

```
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


            try:
                # Create a new contact
                self.ses_client.create_contact(
                    ContactListName=CONTACT_LIST_NAME, EmailAddress=email
                )
                print(f"Contact with email '{email}' created successfully.")

                # Send the welcome email
                self.ses_client.send_email(
                    FromEmailAddress=self.verified_email,
                    Destination={"ToAddresses": [email]},
                    Content={
                        "Simple": {
                            "Subject": {
                                "Data": "Welcome to the Weekly Coupons
 Newsletter"
                            },
                            "Body": {
                                "Text": {"Data": welcome_text},
                                "Html": {"Data": welcome_html},
                            },
                        }
                    },
                )
                print(f"Welcome email sent to '{email}'.")
                if self.sleep:
```

```
                    # 1 email per second in sandbox mode, remove in production.
                    sleep(1.1)
            except ClientError as e:
                # If the contact already exists, skip and proceed
                if e.response["Error"]["Code"] == "AlreadyExistsException":
                    print(f"Contact with email '{email}' already exists.
 Skipping...")
                else:
                    raise e
```

- Pour plus de détails sur l'API, consultez CreateContactle AWS manuel de référence de l'API SDK for Python (Boto3).

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
async fn add_contact(client: &Client, list: &str, email: &str) -> Result<(),
 Error> {
    client
        .create_contact()
        .contact_list_name(list)
        .email_address(email)
        .send()
        .await?;

    println!("Created contact");

    Ok(())
}
```

- Pour plus de détails sur l'API, voir CreateContactla section de référence de l'API AWS SDK for Rust.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`CreateContactList`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`CreateContactList`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Flux de travail des newsletters

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
/// <summary>
/// Creates a contact list with the specified name.
/// </summary>
/// <param name="contactListName">The name of the contact list.</param>
/// <returns>True if successful.</returns>
public async Task<bool> CreateContactListAsync(string contactListName)
{
    var request = new CreateContactListRequest
    {
        ContactListName = contactListName
    };

    try
    {
        var response = await _sesClient.CreateContactListAsync(request);
        return response.HttpStatusCode == HttpStatusCode.OK;
    }
```

```
        catch (AlreadyExistsException ex)
        {
            Console.WriteLine($"Contact list with name {contactListName} already
exists.");
            Console.WriteLine(ex.Message);
            return true;
        }
        catch (LimitExceededException ex)
        {
            Console.WriteLine("The limit for contact lists has been exceeded.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while creating the contact
list: {ex.Message}");
        }
        return false;
    }
```

- Pour plus de détails sur l'API, reportez-vous CreateContactListà la section Référence des AWS SDK for .NET API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    try {
```

```
      // 2. Create a contact list
      String contactListName = CONTACT_LIST_NAME;
      CreateContactListRequest createContactListRequest =
 CreateContactListRequest.builder()
          .contactListName(contactListName)
          .build();
      sesClient.createContactList(createContactListRequest);
      System.out.println("Contact list created: " + contactListName);
    } catch (AlreadyExistsException e) {
      System.out.println("Contact list already exists, skipping creation: weekly-
coupons-newsletter");
    } catch (LimitExceededException e) {
      System.err.println("Limit for contact lists has been exceeded.");
      throw e;
    } catch (SesV2Exception e) {
      System.err.println("Error creating contact list: " + e.getMessage());
      throw e;
    }
```

- Pour plus de détails sur l'API, reportez-vous CreateContactListà la section Référence des AWS SDK for Java 2.x API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
```

```
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


        try:

 self.ses_client.create_contact_list(ContactListName=CONTACT_LIST_NAME)
            print(f"Contact list '{CONTACT_LIST_NAME}' created successfully.")
        except ClientError as e:
            # If the contact list already exists, skip and proceed
            if e.response["Error"]["Code"] == "AlreadyExistsException":
                print(f"Contact list '{CONTACT_LIST_NAME}' already exists.")
            else:
                raise e
```

- Pour plus de détails sur l'API, consultez CreateContactListle AWS manuel de référence de l'API SDK for Python (Boto3).

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
async fn make_list(client: &Client, contact_list: &str) -> Result<(), Error> {
    client
        .create_contact_list()
        .contact_list_name(contact_list)
        .send()
        .await?;

    println!("Created contact list.");

    Ok(())
}
```

- Pour plus de détails sur l'API, voir CreateContactListla section de référence de l'API AWS SDK for Rust.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`CreateEmailIdentity`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`CreateEmailIdentity`.

Les exemples d’actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l’exemple de code suivant :

- Flux de travail des newsletters

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   /// <summary>
   /// Creates an email identity (email address or domain) and starts the
verification process.
   /// </summary>
   /// <param name="emailIdentity">The email address or domain to create and
verify.</param>
   /// <returns>The response from the CreateEmailIdentity operation.</returns>
   public async Task<CreateEmailIdentityResponse>
CreateEmailIdentityAsync(string emailIdentity)
   {
       var request = new CreateEmailIdentityRequest
       {
           EmailIdentity = emailIdentity
       };

       try
       {
           var response = await _sesClient.CreateEmailIdentityAsync(request);
           return response;
       }
       catch (AlreadyExistsException ex)
       {
           Console.WriteLine($"Email identity {emailIdentity} already exists.");
           Console.WriteLine(ex.Message);
           throw;
       }
       catch (ConcurrentModificationException ex)
       {
           Console.WriteLine($"The email identity {emailIdentity} is being
modified by another operation or thread.");
           Console.WriteLine(ex.Message);
           throw;
```

```
        }
        catch (LimitExceededException ex)
        {
            Console.WriteLine("The limit for email identities has been
exceeded.");
            Console.WriteLine(ex.Message);
            throw;
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The email identity {emailIdentity} does not
exist.");
            Console.WriteLine(ex.Message);
            throw;
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
            throw;
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while creating the email
identity: {ex.Message}");
            throw;
        }
    }
```

- Pour plus de détails sur l'API, reportez-vous CreateEmailIdentityà la section Référence des AWS SDK for .NET API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   try {
     CreateEmailIdentityRequest createEmailIdentityRequest =
CreateEmailIdentityRequest.builder()
         .emailIdentity(verifiedEmail)
         .build();
     sesClient.createEmailIdentity(createEmailIdentityRequest);
     System.out.println("Email identity created: " + verifiedEmail);
   } catch (AlreadyExistsException e) {
     System.out.println("Email identity already exists, skipping creation: " +
verifiedEmail);
   } catch (NotFoundException e) {
     System.err.println("The provided email address is not verified: " +
verifiedEmail);
     throw e;
   } catch (LimitExceededException e) {
     System.err
         .println("You have reached the limit for email identities. Please
remove some identities and try again.");
     throw e;
   } catch (SesV2Exception e) {
     System.err.println("Error creating email identity: " + e.getMessage());
     throw e;
   }
```

- Pour plus de détails sur l'API, reportez-vous CreateEmailIdentityà la section Référence des AWS SDK for Java 2.x API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


        try:

 self.ses_client.create_email_identity(EmailIdentity=self.verified_email)
```

```
            print(f"Email identity '{self.verified_email}' created
successfully.")
        except ClientError as e:
            # If the email identity already exists, skip and proceed
            if e.response["Error"]["Code"] == "AlreadyExistsException":
                print(f"Email identity '{self.verified_email}' already exists.")
            else:
                raise e
```

- Pour plus de détails sur l'API, consultez CreateEmailIdentityle AWS manuel de référence de l'API SDK for Python (Boto3).

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
        match self
            .client
            .create_email_identity()
            .email_identity(self.verified_email.clone())
            .send()
            .await
        {
            Ok(_) => writeln!(self.stdout, "Email identity created
successfully.")?,
            Err(e) => match e.into_service_error() {
                CreateEmailIdentityError::AlreadyExistsException(_) => {
                    writeln!(
                        self.stdout,
                        "Email identity already exists, skipping creation."
                    )?;
                }
                e => return Err(anyhow!("Error creating email identity: {}", e)),
            },
```

```
        }
```

- Pour plus de détails sur l'API, voir CreateEmailIdentityla section de référence de l'API AWS SDK for Rust.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`CreateEmailTemplate`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`CreateEmailTemplate`.

Les exemples d’actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l’exemple de code suivant :

- Flux de travail des newsletters

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Creates an email template with the specified content.
    /// </summary>
    /// <param name="templateName">The name of the email template.</param>
    /// <param name="subject">The subject of the email template.</param>
    /// <param name="htmlContent">The HTML content of the email template.</param>
    /// <param name="textContent">The text content of the email template.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> CreateEmailTemplateAsync(string templateName, string
subject, string htmlContent, string textContent)
```

```
    {
        var request = new CreateEmailTemplateRequest
        {
            TemplateName = templateName,
            TemplateContent = new EmailTemplateContent
            {
                Subject = subject,
                Html = htmlContent,
                Text = textContent
            }
        };

        try
        {
            var response = await _sesClient.CreateEmailTemplateAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (AlreadyExistsException ex)
        {
            Console.WriteLine($"Email template with name {templateName} already
exists.");
            Console.WriteLine(ex.Message);
        }
        catch (LimitExceededException ex)
        {
            Console.WriteLine("The limit for email templates has been
exceeded.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while creating the email
template: {ex.Message}");
        }

        return false;
    }
```

- Pour plus de détails sur l'API, reportez-vous CreateEmailTemplateà la section Référence des AWS SDK for .NET API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    try {
      // Create an email template named "weekly-coupons"
      String newsletterHtml = loadFile("resources/coupon_newsletter/coupon-
newsletter.html");
      String newsletterText = loadFile("resources/coupon_newsletter/coupon-
newsletter.txt");

      CreateEmailTemplateRequest templateRequest =
 CreateEmailTemplateRequest.builder()
          .templateName(TEMPLATE_NAME)
          .templateContent(EmailTemplateContent.builder()
              .subject("Weekly Coupons Newsletter")
              .html(newsletterHtml)
              .text(newsletterText)
              .build())
          .build();

      sesClient.createEmailTemplate(templateRequest);

      System.out.println("Email template created: " + TEMPLATE_NAME);
    } catch (AlreadyExistsException e) {
      // If the template already exists, skip this step and proceed with the next
      // operation
      System.out.println("Email template already exists, skipping creation...");
    } catch (LimitExceededException e) {
```

```
      // If the limit for email templates is exceeded, fail the workflow and
 inform
      // the user
      System.err.println("You have reached the limit for email templates. Please
 remove some templates and try again.");
      throw e;
    } catch (Exception e) {
      System.err.println("Error occurred while creating email template: " +
 e.getMessage());
      throw e;
    }
```

- Pour plus de détails sur l'API, reportez-vous CreateEmailTemplateà la section Référence des AWS SDK for Java 2.x API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()
```

```
class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


        try:
            template_content = {
                "Subject": "Weekly Coupons Newsletter",
                "Html": load_file_content("coupon-newsletter.html"),
                "Text": load_file_content("coupon-newsletter.txt"),
            }
            self.ses_client.create_email_template(
                TemplateName=TEMPLATE_NAME, TemplateContent=template_content
            )
            print(f"Email template '{TEMPLATE_NAME}' created successfully.")
        except ClientError as e:
            # If the template already exists, skip and proceed
            if e.response["Error"]["Code"] == "AlreadyExistsException":
                print(f"Email template '{TEMPLATE_NAME}' already exists.")
            else:
                raise e
```

- Pour plus de détails sur l'API, consultez CreateEmailTemplatele AWS manuel de référence de l'API SDK for Python (Boto3).

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
        let template_html =
            std::fs::read_to_string("../resources/newsletter/coupon-
newsletter.html")
                .unwrap_or_else(|_| "Missing coupon-
newsletter.html".to_string());
        let template_text =
            std::fs::read_to_string("../resources/newsletter/coupon-
newsletter.txt")
                .unwrap_or_else(|_| "Missing coupon-newsletter.txt".to_string());

        // Create the email template
        let template_content = EmailTemplateContent::builder()
            .subject("Weekly Coupons Newsletter")
            .html(template_html)
            .text(template_text)
            .build();

        match self
            .client
            .create_email_template()
            .template_name(TEMPLATE_NAME)
            .template_content(template_content)
            .send()
            .await
        {
            Ok(_) => writeln!(self.stdout, "Email template created
 successfully.")?,
            Err(e) => match e.into_service_error() {
                CreateEmailTemplateError::AlreadyExistsException(_) => {
                    writeln!(
                        self.stdout,
                        "Email template already exists, skipping creation."
```

```
                    )?;
                }
                e => return Err(anyhow!("Error creating email template: {}", e)),
            },
        }
```

- Pour plus de détails sur l'API, voir CreateEmailTemplatela section de référence de l'API AWS SDK for Rust.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DeleteContactList`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`DeleteContactList`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Flux de travail des newsletters

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Deletes a contact list and all contacts within it.
    /// </summary>
    /// <param name="contactListName">The name of the contact list to delete.</
param>
```

```
    /// <returns>True if successful.</returns>
    public async Task<bool> DeleteContactListAsync(string contactListName)
    {
        var request = new DeleteContactListRequest
        {
            ContactListName = contactListName
        };

        try
        {
            var response = await _sesClient.DeleteContactListAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (ConcurrentModificationException ex)
        {
            Console.WriteLine($"The contact list {contactListName} is being
modified by another operation or thread.");
            Console.WriteLine(ex.Message);
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The contact list {contactListName} does not
exist.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while deleting the contact
list: {ex.Message}");
        }

        return false;
    }
```

- Pour plus de détails sur l'API, reportez-vous DeleteContactListà la section Référence des AWS SDK for .NET API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   try {
     // Delete the contact list
     DeleteContactListRequest deleteContactListRequest =
DeleteContactListRequest.builder()
         .contactListName(CONTACT_LIST_NAME)
         .build();

     sesClient.deleteContactList(deleteContactListRequest);

     System.out.println("Contact list deleted: " + CONTACT_LIST_NAME);
   } catch (NotFoundException e) {
     // If the contact list does not exist, log the error and proceed
     System.out.println("Contact list not found. Skipping deletion...");
   } catch (Exception e) {
     System.err.println("Error occurred while deleting the contact list: " +
e.getMessage());
     e.printStackTrace();
   }
```

- Pour plus de détails sur l'API, reportez-vous DeleteContactListà la section Référence des AWS SDK for Java 2.x API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


        try:

 self.ses_client.delete_contact_list(ContactListName=CONTACT_LIST_NAME)
            print(f"Contact list '{CONTACT_LIST_NAME}' deleted successfully.")
```

```
        except ClientError as e:
            # If the contact list doesn't exist, skip and proceed
            if e.response["Error"]["Code"] == "NotFoundException":
                print(f"Contact list '{CONTACT_LIST_NAME}' does not exist.")
            else:
                print(e)
```

- Pour plus de détails sur l'API, consultez DeleteContactListle AWS manuel de référence de l'API SDK for Python (Boto3).

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
        match self
            .client
            .delete_contact_list()
            .contact_list_name(CONTACT_LIST_NAME)
            .send()
            .await
        {
            Ok(_) => writeln!(self.stdout, "Contact list deleted
successfully.")?,
            Err(e) => return Err(anyhow!("Error deleting contact list: {e}")),
        }
```

- Pour plus de détails sur l'API, voir DeleteContactListla section de référence de l'API AWS SDK for Rust.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DeleteEmailIdentity`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`DeleteEmailIdentity`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Flux de travail des newsletters

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Deletes an email identity (email address or domain).
    /// </summary>
    /// <param name="emailIdentity">The email address or domain to delete.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> DeleteEmailIdentityAsync(string emailIdentity)
    {
        var request = new DeleteEmailIdentityRequest
        {
            EmailIdentity = emailIdentity
        };

        try
        {
            var response = await _sesClient.DeleteEmailIdentityAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (ConcurrentModificationException ex)
        {
```

```
            Console.WriteLine($"The email identity {emailIdentity} is being
modified by another operation or thread.");
            Console.WriteLine(ex.Message);
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The email identity {emailIdentity} does not
exist.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while deleting the email
identity: {ex.Message}");
        }

        return false;
    }
```

- Pour plus de détails sur l'API, reportez-vous DeleteEmailIdentityà la section Référence des AWS SDK for .NET API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    try {
      // Delete the email identity
```

```
        DeleteEmailIdentityRequest deleteIdentityRequest =
 DeleteEmailIdentityRequest.builder()
            .emailIdentity(this.verifiedEmail)
            .build();

        sesClient.deleteEmailIdentity(deleteIdentityRequest);

        System.out.println("Email identity deleted: " + this.verifiedEmail);
      } catch (NotFoundException e) {
        // If the email identity does not exist, log the error and proceed
        System.out.println("Email identity not found. Skipping deletion...");
      } catch (Exception e) {
        System.err.println("Error occurred while deleting the email identity: " +
e.getMessage());
        e.printStackTrace();
      }
    } else {
      System.out.println("Skipping email identity deletion.");
    }
```

- Pour plus de détails sur l'API, reportez-vous DeleteEmailIdentityà la section Référence des AWS SDK for Java 2.x API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
```

```
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


            try:

 self.ses_client.delete_email_identity(EmailIdentity=self.verified_email)
                print(f"Email identity '{self.verified_email}' deleted
 successfully.")
            except ClientError as e:
                # If the email identity doesn't exist, skip and proceed
                if e.response["Error"]["Code"] == "NotFoundException":
                    print(f"Email identity '{self.verified_email}' does not
 exist.")
                else:
                    print(e)
```

- Pour plus de détails sur l'API, consultez DeleteEmailIdentityle AWS manuel de référence de l'API SDK for Python (Boto3).

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
            match self
                .client
                .delete_email_identity()
                .email_identity(self.verified_email.clone())
                .send()
                .await
            {
                Ok(_) => writeln!(self.stdout, "Email identity deleted
successfully.")?,
                Err(e) => {
                    return Err(anyhow!("Error deleting email identity: {}", e));
                }
            }
```

- Pour plus de détails sur l'API, voir DeleteEmailIdentityla section de référence de l'API AWS SDK for Rust.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DeleteEmailTemplate`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`DeleteEmailTemplate`.

Les exemples d’actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l’exemple de code suivant :

- Flux de travail des newsletters

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Deletes an email template.
    /// </summary>
    /// <param name="templateName">The name of the email template to delete.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> DeleteEmailTemplateAsync(string templateName)
    {
        var request = new DeleteEmailTemplateRequest
        {
            TemplateName = templateName
        };

        try
        {
            var response = await _sesClient.DeleteEmailTemplateAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The email template {templateName} does not
 exist.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
 later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
```

```
            Console.WriteLine($"An error occurred while deleting the email
template: {ex.Message}");
        }

        return false;
    }
```

- Pour plus de détails sur l'API, reportez-vous DeleteEmailTemplateà la section Référence des AWS SDK for .NET API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    try {
      // Delete the template
      DeleteEmailTemplateRequest deleteTemplateRequest =
DeleteEmailTemplateRequest.builder()
          .templateName(TEMPLATE_NAME)
          .build();

      sesClient.deleteEmailTemplate(deleteTemplateRequest);

      System.out.println("Email template deleted: " + TEMPLATE_NAME);
    } catch (NotFoundException e) {
      // If the email template does not exist, log the error and proceed
      System.out.println("Email template not found. Skipping deletion...");
    } catch (Exception e) {
      System.err.println("Error occurred while deleting the email template: " +
e.getMessage());
      e.printStackTrace();
    }
```

- Pour plus de détails sur l'API, reportez-vous DeleteEmailTemplateà la section Référence des AWS SDK for Java 2.x API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep
```

```
        try:
            self.ses_client.delete_email_template(TemplateName=TEMPLATE_NAME)
            print(f"Email template '{TEMPLATE_NAME}' deleted successfully.")
        except ClientError as e:
            # If the email template doesn't exist, skip and proceed
            if e.response["Error"]["Code"] == "NotFoundException":
                print(f"Email template '{TEMPLATE_NAME}' does not exist.")
            else:
                print(e)
```

- Pour plus de détails sur l'API, consultez DeleteEmailTemplatele AWS manuel de référence de l'API SDK for Python (Boto3).

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
        match self
            .client
            .delete_email_template()
            .template_name(TEMPLATE_NAME)
            .send()
            .await
        {
            Ok(_) => writeln!(self.stdout, "Email template deleted
successfully.")?,
            Err(e) => {
                return Err(anyhow!("Error deleting email template: {e}"));
            }
        }
```

- Pour plus de détails sur l'API, voir DeleteEmailTemplatela section de référence de l'API AWS SDK for Rust.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`GetEmailIdentity`** avec un AWS SDK ou une CLI

L'exemple de code suivant montre comment utiliser`GetEmailIdentity`.

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Détermine si une adresse e-mail a été vérifiée.

```
async fn is_verified(client: &Client, email: &str) -> Result<(), Error> {
    let resp = client
        .get_email_identity()
        .email_identity(email)
        .send()
        .await?;

    if resp.verified_for_sending_status() {
        println!("The address is verified");
    } else {
        println!("The address is not verified");
    }

    Ok(())
}
```

- Pour plus de détails sur l'API, voir GetEmailIdentityla section de référence de l'API AWS SDK for Rust.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`ListContactLists`** avec un AWS SDK ou une CLI

L'exemple de code suivant montre comment utiliser`ListContactLists`.

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
async fn show_lists(client: &Client) -> Result<(), Error> {
    let resp = client.list_contact_lists().send().await?;

    println!("Contact lists:");

    for list in resp.contact_lists() {
        println!("  {}", list.contact_list_name().unwrap_or_default());
    }

    Ok(())
}
```

- Pour plus de détails sur l'API, voir ListContactListsla section de référence de l'API AWS SDK for Rust.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`ListContacts`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`ListContacts`.

Les exemples d'actions sont des extraits de code de programmes de plus grande envergure et doivent être exécutés en contexte. Vous pouvez voir cette action en contexte dans l'exemple de code suivant :

- Flux de travail des newsletters

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Lists the contacts in the specified contact list.
    /// </summary>
    /// <param name="contactListName">The name of the contact list.</param>
    /// <returns>The list of contacts response from the ListContacts operation.</
returns>
    public async Task<List<Contact>> ListContactsAsync(string contactListName)
    {
        var request = new ListContactsRequest
        {
            ContactListName = contactListName
        };

        try
        {
            var response = await _sesClient.ListContactsAsync(request);
            return response.Contacts;
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The contact list {contactListName} does not
 exist.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
```

```
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while listing the contacts:
{ex.Message}");
        }

        return new List<Contact>();
    }
```

- Pour plus de détails sur l'API, reportez-vous ListContactsà la section Référence des AWS SDK for .NET API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
     ListContactsRequest contactListRequest = ListContactsRequest.builder()
         .contactListName(CONTACT_LIST_NAME)
         .build();

     List<String> contactEmails;
     try {
       ListContactsResponse contactListResponse =
sesClient.listContacts(contactListRequest);

       contactEmails = contactListResponse.contacts().stream()
           .map(Contact::emailAddress)
           .toList();
     } catch (Exception e) {
```

```
        // TODO: Remove when listContacts's GET body issue is resolved.
        contactEmails = this.contacts;
      }
```

- Pour plus de détails sur l'API, reportez-vous ListContactsà la section Référence des AWS SDK for Java 2.x API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """
```

```
    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


        try:
            contacts_response = self.ses_client.list_contacts(
                ContactListName=CONTACT_LIST_NAME
            )
        except ClientError as e:
            if e.response["Error"]["Code"] == "NotFoundException":
                print(f"Contact list '{CONTACT_LIST_NAME}' does not exist.")
                return
            else:
                raise e
```

- Pour plus de détails sur l'API, consultez ListContactsle AWS manuel de référence de l'API SDK for Python (Boto3).

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
async fn show_contacts(client: &Client, list: &str) -> Result<(), Error> {
    let resp = client
        .list_contacts()
        .contact_list_name(list)
        .send()
        .await?;

    println!("Contacts:");

    for contact in resp.contacts() {
```

```
        println!("  {}", contact.email_address().unwrap_or_default());
    }

    Ok(())
}
```

- Pour plus de détails sur l'API, voir ListContactsla section de référence de l'API AWS SDK for Rust.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`SendEmail`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`SendEmail`.

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Sends an email with the specified content and options.
    /// </summary>
    /// <param name="fromEmailAddress">The email address to send the email
from.</param>
    /// <param name="toEmailAddresses">The email addresses to send the email
to.</param>
    /// <param name="subject">The subject of the email.</param>
    /// <param name="htmlContent">The HTML content of the email.</param>
    /// <param name="textContent">The text content of the email.</param>
    /// <param name="templateName">The name of the email template to use
(optional).</param>
```

```
   /// <param name="templateData">The data to replace placeholders in the email
template (optional).</param>
   /// <param name="contactListName">The name of the contact list for
unsubscribe functionality (optional).</param>
   /// <returns>The MessageId response from the SendEmail operation.</returns>
   public async Task<string> SendEmailAsync(string fromEmailAddress,
List<string> toEmailAddresses, string? subject,
       string? htmlContent, string? textContent, string? templateName = null,
string? templateData = null, string? contactListName = null)
   {
       var request = new SendEmailRequest
       {
           FromEmailAddress = fromEmailAddress
       };

       if (toEmailAddresses.Any())
       {
           request.Destination = new Destination { ToAddresses =
toEmailAddresses };
       }

       if (!string.IsNullOrEmpty(templateName))
       {
           request.Content = new EmailContent()
           {
               Template = new Template
               {
                   TemplateName = templateName,
                   TemplateData = templateData
               }
           };
       }
       else
       {
           request.Content = new EmailContent
           {
               Simple = new Message
               {
                   Subject = new Content { Data = subject },
                   Body = new Body
                   {
                       Html = new Content { Data = htmlContent },
                       Text = new Content { Data = textContent }
                   }
```

```
                }
            };
        }

        if (!string.IsNullOrEmpty(contactListName))
        {
            request.ListManagementOptions = new ListManagementOptions
            {
                ContactListName = contactListName
            };
        }

        try
        {
            var response = await _sesClient.SendEmailAsync(request);
            return response.MessageId;
        }
        catch (AccountSuspendedException ex)
        {
            Console.WriteLine("The account's ability to send email has been
permanently restricted.");
            Console.WriteLine(ex.Message);
        }
        catch (MailFromDomainNotVerifiedException ex)
        {
            Console.WriteLine("The sending domain is not verified.");
            Console.WriteLine(ex.Message);
        }
        catch (MessageRejectedException ex)
        {
            Console.WriteLine("The message content is invalid.");
            Console.WriteLine(ex.Message);
        }
        catch (SendingPausedException ex)
        {
            Console.WriteLine("The account's ability to send email is currently
paused.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
```

```
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while sending the email:
{ex.Message}");
        }

        return string.Empty;
    }
```

- Pour plus de détails sur l'API, reportez-vous SendEmailà la section Référence des AWS SDK for .NET API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Envoie un message.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.sesv2.model.Body;
import software.amazon.awssdk.services.sesv2.model.Content;
import software.amazon.awssdk.services.sesv2.model.Destination;
import software.amazon.awssdk.services.sesv2.model.EmailContent;
import software.amazon.awssdk.services.sesv2.model.Message;
import software.amazon.awssdk.services.sesv2.model.SendEmailRequest;
import software.amazon.awssdk.services.sesv2.model.SesV2Exception;
import software.amazon.awssdk.services.sesv2.SesV2Client;

/**
 * Before running this AWS SDK for Java (v2) example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
```

```
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class SendEmail {
        public static void main(String[] args) {
                final String usage = """

                                Usage:
                                    <sender> <recipient> <subject>\s

                                Where:
                                    sender - An email address that represents the
 sender.\s
                                    recipient - An email address that represents
 the recipient.\s
                                    subject - The subject line.\s
                                """;

                if (args.length != 3) {
                        System.out.println(usage);
                        System.exit(1);
                }

                String sender = args[0];
                String recipient = args[1];
                String subject = args[2];

                Region region = Region.US_EAST_1;
                SesV2Client sesv2Client = SesV2Client.builder()
                                .region(region)
                                .build();

                // The HTML body of the email.
                String bodyHTML = "<html>" + "<head></head>" + "<body>" +
 "<h1>Hello!</h1>"
                                + "<p> See the list of customers.</p>" + "</
body>" + "</html>";

                send(sesv2Client, sender, recipient, subject, bodyHTML);
        }

        public static void send(SesV2Client client,
                        String sender,
```

```
                        String recipient,
                        String subject,
                        String bodyHTML) {

                Destination destination = Destination.builder()
                                .toAddresses(recipient)
                                .build();

                Content content = Content.builder()
                                .data(bodyHTML)
                                .build();

                Content sub = Content.builder()
                                .data(subject)
                                .build();

                Body body = Body.builder()
                                .html(content)
                                .build();

                Message msg = Message.builder()
                                .subject(sub)
                                .body(body)
                                .build();

                EmailContent emailContent = EmailContent.builder()
                                .simple(msg)
                                .build();

                SendEmailRequest emailRequest = SendEmailRequest.builder()
                                .destination(destination)
                                .content(emailContent)
                                .fromEmailAddress(sender)
                                .build();

                try {
                        System.out.println("Attempting to send an email through
Amazon SES "
                                        + "using the AWS SDK for Java...");
                        client.sendEmail(emailRequest);
                        System.out.println("email was sent");

                } catch (SesV2Exception e) {
                        System.err.println(e.awsErrorDetails().errorMessage());
```

```
                        System.exit(1);
                }
        }
}
```

Envoie un message à l'aide d'un modèle.

```
      String coupons = Files.readString(Paths.get("resources/coupon_newsletter/
sample_coupons.json"));
      for (String emailAddress : contactEmails) {
        SendEmailRequest newsletterRequest = SendEmailRequest.builder()
            .destination(Destination.builder().toAddresses(emailAddress).build())
            .content(EmailContent.builder()
                .template(Template.builder()
                    .templateName(TEMPLATE_NAME)
                    .templateData(coupons)
                    .build())
                .build())
            .fromEmailAddress(this.verifiedEmail)
            .listManagementOptions(ListManagementOptions.builder()
                .contactListName(CONTACT_LIST_NAME)
                .build())
            .build();
        SendEmailResponse newsletterResponse =
 sesClient.sendEmail(newsletterRequest);
        System.out.println("Newsletter sent to " + emailAddress + ": " +
 newsletterResponse.messageId());
      }
```

- Pour plus de détails sur l'API, reportez-vous SendEmailà la section Référence des AWS SDK for Java 2.x API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Envoie un message à tous les membres de la liste de contacts.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


                self.ses_client.send_email(
                    FromEmailAddress=self.verified_email,
                    Destination={"ToAddresses": [email]},
```

```
                    Content={
                        "Simple": {
                            "Subject": {
                                "Data": "Welcome to the Weekly Coupons
 Newsletter"
                            },
                            "Body": {
                                "Text": {"Data": welcome_text},
                                "Html": {"Data": welcome_html},
                            },
                        }
                    },
                )
                print(f"Welcome email sent to '{email}'.")
```

Envoie un message à tous les membres de la liste de contacts à l'aide d'un modèle.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
```

```
        self.sleep = sleep


                self.ses_client.send_email(
                    FromEmailAddress=self.verified_email,
                    Destination={"ToAddresses": [email_address]},
                    Content={
                        "Template": {
                            "TemplateName": TEMPLATE_NAME,
                            "TemplateData": coupon_items,
                        }
                    },
                    ListManagementOptions={"ContactListName": CONTACT_LIST_NAME},
                )
```

- Pour plus de détails sur l'API, consultez SendEmaille AWS manuel de référence de l'API SDK for Python (Boto3).

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
require "aws-sdk-sesv2"
require_relative "config" # Recipient and sender email addresses.

# Set up the SESv2 client.
client = Aws::SESV2::Client.new(region: AWS_REGION)

def send_email(client, sender_email, recipient_email)
  response = client.send_email(
    {
       from_email_address: sender_email,
       destination: {
         to_addresses: [recipient_email]
```

```
      },
      content: {
        simple: {
          subject: {
            data: "Test email subject"
          },
          body: {
            text: {
              data: "Test email body"
            }
          }
        }
      }
    }
  )
  puts "Email sent from #{SENDER_EMAIL} to #{RECIPIENT_EMAIL} with message ID:
 #{response.message_id}"
end

send_email(client, SENDER_EMAIL, RECIPIENT_EMAIL)
```

- Pour plus de détails sur l'API, reportez-vous SendEmailà la section Référence des AWS SDK for Ruby API.

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Envoie un message à tous les membres de la liste de contacts.

```
async fn send_message(
    client: &Client,
    list: &str,
    from: &str,
    subject: &str,
```

```
    message: &str,
) -> Result<(), Error> {
    // Get list of email addresses from contact list.
    let resp = client
        .list_contacts()
        .contact_list_name(list)
        .send()
        .await?;

    let contacts = resp.contacts();

    let cs: Vec<String> = contacts
        .iter()
        .map(|i| i.email_address().unwrap_or_default().to_string())
        .collect();

    let mut dest: Destination = Destination::builder().build();
    dest.to_addresses = Some(cs);
    let subject_content = Content::builder()
        .data(subject)
        .charset("UTF-8")
        .build()
        .expect("building Content");
    let body_content = Content::builder()
        .data(message)
        .charset("UTF-8")
        .build()
        .expect("building Content");
    let body = Body::builder().text(body_content).build();

    let msg = Message::builder()
        .subject(subject_content)
        .body(body)
        .build();

    let email_content = EmailContent::builder().simple(msg).build();

    client
        .send_email()
        .from_email_address(from)
        .destination(dest)
        .content(email_content)
        .send()
        .await?;
```

```
    println!("Email sent to list");

    Ok(())
}
```

Envoie un message à tous les membres de la liste de contacts à l'aide d'un modèle.

```
            let coupons = std::fs::read_to_string("../resources/newsletter/
sample_coupons.json")
                .unwrap_or_else(|_| r#"{"coupons":[]}"#.to_string());
            let email_content = EmailContent::builder()
                .template(
                    Template::builder()
                        .template_name(TEMPLATE_NAME)
                        .template_data(coupons)
                        .build(),
                )
                .build();

            match self
                .client
                .send_email()
                .from_email_address(self.verified_email.clone())

 .destination(Destination::builder().to_addresses(email.clone()).build())
                .content(email_content)
                .list_management_options(
                    ListManagementOptions::builder()
                        .contact_list_name(CONTACT_LIST_NAME)
                        .build()?,
                )
                .send()
                .await
            {
                Ok(output) => {
                    if let Some(message_id) = output.message_id {
                        writeln!(
                            self.stdout,
                            "Newsletter sent to {} with message ID {}",
                            email, message_id
                        )?;
```

```
                    } else {
                        writeln!(self.stdout, "Newsletter sent to {}", email)?;
                    }
                }
                Err(e) => return Err(anyhow!("Error sending newsletter to {}:
{}", email, e)),
            }
```

- Pour plus de détails sur l'API, voir SendEmailla section de référence de l'API AWS SDK for Rust.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Scénarios pour l'API Amazon SES v2 à l'aide de AWS kits SDK

Les exemples de code suivants vous montrent comment implémenter des scénarios courants dans l'API Amazon SES v2 avec des AWS SDK. Ces scénarios vous montrent comment accomplir des tâches spécifiques en appelant plusieurs fonctions au sein de l'API Amazon SES v2. Chaque scénario inclut un lien vers GitHub, où vous pouvez trouver des instructions sur la façon de configurer et d'exécuter le code.

Exemples

- Un flux de newsletter complet sur l'API Amazon SES v2 à l'aide d'un AWS SDK

Un flux de newsletter complet sur l'API Amazon SES v2 à l'aide d'un AWS SDK

Les exemples de code suivants montrent comment exécuter le flux de newsletter de l'API Amazon SES v2.

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Exécutez le flux de travail.

```
using System.Diagnostics;
using System.Text.RegularExpressions;
using Amazon.SimpleEmailV2;
using Amazon.SimpleEmailV2.Model;
using Microsoft.Extensions.DependencyInjection;
using Microsoft.Extensions.Hosting;
using Microsoft.Extensions.Logging;
using Microsoft.Extensions.Logging.Console;
using Microsoft.Extensions.Logging.Debug;

namespace Sesv2Scenario;

public static class NewsletterWorkflow
{
    /*
      This workflow demonstrates how to use the Amazon Simple Email Service (SES)
 v2 to send a coupon newsletter to a list of subscribers.
      The workflow performs the following tasks:

      1. Prepare the application:
         - Create a verified email identity for sending and replying to emails.
         - Create a contact list to store the subscribers' email addresses.
         - Create an email template for the coupon newsletter.

      2. Gather subscriber email addresses:
         - Prompt the user for a base email address.
         - Create 3 variants of the email address using subaddress extensions
 (e.g., user+ses-weekly-newsletter-1@example.com).
         - Add each variant as a contact to the contact list.
         - Send a welcome email to each new contact.
```

```
      3. Send the coupon newsletter:
         - Retrieve the list of contacts from the contact list.
         - Send the coupon newsletter using the email template to each contact.

      4. Monitor and review:
         - Provide instructions for the user to review the sending activity and
 metrics in the AWS console.

      5. Clean up resources:
         - Delete the contact list (which also deletes all contacts within it).
         - Delete the email template.
         - Optionally delete the verified email identity.

   */

   public static SESv2Wrapper _sesv2Wrapper;
   public static string? _baseEmailAddress = null;
   public static string? _verifiedEmail = null;
   private static string _contactListName = "weekly-coupons-newsletter";
   private static string _templateName = "weekly-coupons";
   private static string _subject = "Weekly Coupons Newsletter";
   private static string _htmlContentFile = "coupon-newsletter.html";
   private static string _textContentFile = "coupon-newsletter.txt";
   private static string _htmlWelcomeFile = "welcome.html";
   private static string _textWelcomeFile = "welcome.txt";
   private static string _couponsDataFile = "sample_coupons.json";

   // Relative location of the shared workflow resources folder.
   private static string _resourcesFilePathLocation = "../../../../../../../
workflows/sesv2_weekly_mailer/resources/";

   public static async Task Main(string[] args)
   {
       // Set up dependency injection for the Amazon service.
       using var host = Host.CreateDefaultBuilder(args)
           .ConfigureLogging(logging =>
               logging.AddFilter("System", LogLevel.Debug)
                   .AddFilter<DebugLoggerProvider>("Microsoft",
 LogLevel.Information)
                   .AddFilter<ConsoleLoggerProvider>("Microsoft",
 LogLevel.Trace))
           .ConfigureServices((_, services) =>
               services.AddAWSService<IAmazonSimpleEmailServiceV2>()
                   .AddTransient<SESv2Wrapper>()
```

```
            )
            .Build();

        ServicesSetup(host);

        try
        {
            Console.WriteLine(new string('-', 80));
            Console.WriteLine(new string('-', 80));
            Console.WriteLine("Welcome to the Amazon SES v2 Coupon Newsletter
Workflow.");
            Console.WriteLine("This workflow demonstrates how to use the Amazon
Simple Email Service (SES) v2 " +
                              "\r\nto send a coupon newsletter to a list of
subscribers.");

            // Prepare the application.
            var emailIdentity = await PrepareApplication();

            // Gather subscriber email addresses.
            await GatherSubscriberEmailAddresses(emailIdentity);

            // Send the coupon newsletter.
            await SendCouponNewsletter(emailIdentity);

            // Monitor and review.
            MonitorAndReview(true);

            // Clean up resources.
            await Cleanup(emailIdentity, true);

            Console.WriteLine(new string('-', 80));
            Console.WriteLine("Amazon SES v2 Coupon Newsletter Workflow is
complete.");
            Console.WriteLine(new string('-', 80));
            Console.WriteLine(new string('-', 80));
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred: {ex.Message}");
        }
    }

    /// <summary>
```

```
    /// Populate the services for use within the console application.
    /// </summary>
    /// <param name="host">The services host.</param>
    private static void ServicesSetup(IHost host)
    {
        _sesv2Wrapper = host.Services.GetRequiredService<SESv2Wrapper>();
    }

    /// <summary>
    /// Set up the resources for the workflow.
    /// </summary>
    /// <returns>The email address of the verified identity.</returns>
    public static async Task<string?> PrepareApplication()
    {
        var htmlContent = await File.ReadAllTextAsync(_resourcesFilePathLocation
+ _htmlContentFile);
        var textContent = await File.ReadAllTextAsync(_resourcesFilePathLocation
+ _textContentFile);

        Console.WriteLine(new string('-', 80));
        Console.WriteLine("1. In this step, we will prepare the application:" +
                          "\r\n  - Create a verified email identity for sending
and replying to emails." +
                          "\r\n  - Create a contact list to store the
subscribers' email addresses." +
                          "\r\n  - Create an email template for the coupon
newsletter.\r\n");

        // Prompt the user for a verified email address.
        while (!IsEmail(_verifiedEmail))
        {
            Console.Write("Enter a verified email address or an email to verify:
");
            _verifiedEmail = Console.ReadLine();
        }

        try
        {
            // Create an email identity and start the verification process.
            await _sesv2Wrapper.CreateEmailIdentityAsync(_verifiedEmail);
            Console.WriteLine($"Identity {_verifiedEmail} created.");
        }
        catch (AlreadyExistsException)
        {
```

```
            Console.WriteLine($"Identity {_verifiedEmail} already exists.");
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Error creating email identity: {ex.Message}");
        }

        // Create a contact list.
        try
        {
            await _sesv2Wrapper.CreateContactListAsync(_contactListName);
            Console.WriteLine($"Contact list {_contactListName} created.");
        }
        catch (AlreadyExistsException)
        {
            Console.WriteLine($"Contact list {_contactListName} already
exists.");
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Error creating contact list: {ex.Message}");
        }

        // Create an email template.
        try
        {
            await _sesv2Wrapper.CreateEmailTemplateAsync(_templateName, _subject,
htmlContent, textContent);
            Console.WriteLine($"Email template {_templateName} created.");
        }
        catch (AlreadyExistsException)
        {
            Console.WriteLine($"Email template {_templateName} already exists.");
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Error creating email template: {ex.Message}");
        }

        return _verifiedEmail;
    }

    /// <summary>
    /// Generate subscriber addresses and send welcome emails.
```

```
    /// </summary>
    /// <param name="fromEmailAddress">The verified email address from
 PrepareApplication.</param>
    /// <returns>True if successful.</returns>
    public static async Task<bool> GatherSubscriberEmailAddresses(string
 fromEmailAddress)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine("2. In Step 2, we will gather subscriber email
 addresses:" +
                          "\r\n  - Prompt the user for a base email address." +
                          "\r\n  - Create 3 variants of the email address using
 subaddress extensions (e.g., user+ses-weekly-newsletter-1@example.com)." +
                          "\r\n  - Add each variant as a contact to the contact
 list." +
                          "\r\n  - Send a welcome email to each new contact.\r
\n");

        // Prompt the user for a base email address.
        while (!IsEmail(_baseEmailAddress))
        {
            Console.Write("Enter a base email address (e.g., user@example.com):
 ");
            _baseEmailAddress = Console.ReadLine();
        }

        // Create 3 variants of the email address using +ses-weekly-newsletter-1,
 +ses-weekly-newsletter-2, etc.
        var baseEmailAddressParts = _baseEmailAddress!.Split("@");
        for (int i = 1; i <= 3; i++)
        {
            string emailAddress = $"{baseEmailAddressParts[0]}+ses-weekly-
newsletter-{i}@{baseEmailAddressParts[1]}";

            try
            {
                // Create a contact with the email address in the contact list.
                await _sesv2Wrapper.CreateContactAsync(emailAddress,
 _contactListName);
                Console.WriteLine($"Contact {emailAddress} added to the
 {_contactListName} contact list.");
            }
            catch (AlreadyExistsException)
            {
```

```
                Console.WriteLine($"Contact {emailAddress} already exists in the
{_contactListName} contact list.");
            }
            catch (Exception ex)
            {
                Console.WriteLine($"Error creating contact {emailAddress}:
{ex.Message}");
                return false;
            }

            // Send a welcome email to the new contact.
            try
            {
                string subject = "Welcome to the Weekly Coupons Newsletter";
                string htmlContent = await
File.ReadAllTextAsync(_resourcesFilePathLocation + _htmlWelcomeFile);
                string textContent = await
File.ReadAllTextAsync(_resourcesFilePathLocation + _textWelcomeFile);

                await _sesv2Wrapper.SendEmailAsync(fromEmailAddress, new
List<string> { emailAddress }, subject, htmlContent, textContent);
                Console.WriteLine($"Welcome email sent to {emailAddress}.");
            }
            catch (Exception ex)
            {
                Console.WriteLine($"Error sending welcome email to
{emailAddress}: {ex.Message}");
                return false;
            }

            // Wait 2 seconds before sending the next email (if the account is in
the SES Sandbox).
            await Task.Delay(2000);
        }

        return true;
    }

    /// <summary>
    ///  Send the coupon newsletter to the subscribers in the contact list.
    /// </summary>
    /// <param name="fromEmailAddress">The verified email address from
PrepareApplication.</param>
    /// <returns>True if successful.</returns>
```

```
   public static async Task<bool> SendCouponNewsletter(string fromEmailAddress)
   {
       Console.WriteLine(new string('-', 80));
       Console.WriteLine("3. In this step, we will send the coupon newsletter:"
+
                         "\r\n  - Retrieve the list of contacts from the contact
list." +
                         "\r\n  - Send the coupon newsletter using the email
template to each contact.\r\n");


       // Retrieve the list of contacts from the contact list.
       var contacts = await _sesv2Wrapper.ListContactsAsync(_contactListName);
       if (!contacts.Any())
       {
           Console.WriteLine($"No contacts found in the {_contactListName}
contact list.");
           return false;
       }

       // Load the coupon data from the sample_coupons.json file.
       string couponsData = await
File.ReadAllTextAsync(_resourcesFilePathLocation + _couponsDataFile);

       // Send the coupon newsletter to each contact using the email template.
       try
       {
           foreach (var contact in contacts)
           {
               // To use the Contact List for list management, send to only one
address at a time.
               await _sesv2Wrapper.SendEmailAsync(fromEmailAddress,
                   new List<string> { contact.EmailAddress },
                   null, null, null, _templateName, couponsData,
_contactListName);
           }

           Console.WriteLine($"Coupon newsletter sent to contact list
{_contactListName}.");
       }
       catch (Exception ex)
       {
           Console.WriteLine($"Error sending coupon newsletter to contact list
{_contactListName}: {ex.Message}");
```

```
            return false;
        }

        return true;
    }

    /// <summary>
    /// Provide instructions for monitoring sending activity and metrics.
    /// </summary>
    /// <param name="interactive">True to run in interactive mode.</param>
    /// <returns>True if successful.</returns>
    public static bool MonitorAndReview(bool interactive)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine("4. In step 4, we will monitor and review:" +
                          "\r\n  - Provide instructions for the user to review
the sending activity and metrics in the AWS console.\r\n");

        Console.WriteLine("Review your sending activity using the SES Homepage in
the AWS console.");
        Console.WriteLine("Press Enter to open the SES Homepage in your default
browser...");
        if (interactive)
        {
            Console.ReadLine();
            try
            {
                // Open the SES Homepage in the default browser.
                Process.Start(new ProcessStartInfo
                {
                    FileName = "https://console.aws.amazon.com/ses/home",
                    UseShellExecute = true
                });
            }
            catch (Exception ex)
            {
                Console.WriteLine($"Error opening the SES Homepage:
{ex.Message}");
                return false;
            }
        }

        Console.WriteLine("Review the sending activity and email metrics, then
press Enter to continue...");
```

```
        if (interactive)
            Console.ReadLine();
        return true;
    }

    /// <summary>
    /// Clean up the resources used in the workflow.
    /// </summary>
    /// <param name="verifiedEmailAddress">The verified email address from
 PrepareApplication.</param>
    /// <param name="interactive">True if interactive.</param>
    /// <returns>Async task.</returns>
    public static async Task<bool> Cleanup(string verifiedEmailAddress, bool
 interactive)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine("5. Finally, we clean up resources:" +
                          "\r\n  - Delete the contact list (which also deletes
 all contacts within it)." +
                          "\r\n  - Delete the email template." +
                          "\r\n  - Optionally delete the verified email identity.
\r\n");

        Console.WriteLine("Cleaning up resources...");

        // Delete the contact list (this also deletes all contacts in the list).
        try
        {
            await _sesv2Wrapper.DeleteContactListAsync(_contactListName);
            Console.WriteLine($"Contact list {_contactListName} deleted.");
        }
        catch (NotFoundException)
        {
            Console.WriteLine($"Contact list {_contactListName} not found.");
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Error deleting contact list {_contactListName}:
 {ex.Message}");
            return false;
        }

        // Delete the email template.
        try
```

```
        {
            await _sesv2Wrapper.DeleteEmailTemplateAsync(_templateName);
            Console.WriteLine($"Email template {_templateName} deleted.");
        }
        catch (NotFoundException)
        {
            Console.WriteLine($"Email template {_templateName} not found.");
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Error deleting email template {_templateName}:
{ex.Message}");
            return false;
        }

        // Ask the user if they want to delete the email identity.
        var deleteIdentity = !interactive ||
            GetYesNoResponse(
                $"Do you want to delete the email identity
{verifiedEmailAddress}? (y/n) ");
        if (deleteIdentity)
        {
            try
            {
                await
_sesv2Wrapper.DeleteEmailIdentityAsync(verifiedEmailAddress);
                Console.WriteLine($"Email identity {verifiedEmailAddress}
deleted.");
            }
            catch (NotFoundException)
            {
                Console.WriteLine(
                    $"Email identity {verifiedEmailAddress} not found.");
            }
            catch (Exception ex)
            {
                Console.WriteLine(
                    $"Error deleting email identity {verifiedEmailAddress}:
{ex.Message}");
                return false;
            }
        }
        else
        {
```

```
            Console.WriteLine(
                $"Skipping deletion of email identity {verifiedEmailAddress}.");
        }

        return true;
    }

    /// <summary>
    /// Helper method to get a yes or no response from the user.
    /// </summary>
    /// <param name="question">The question string to print on the console.</
param>
    /// <returns>True if the user responds with a yes.</returns>
    private static bool GetYesNoResponse(string question)
    {
        Console.WriteLine(question);
        var ynResponse = Console.ReadLine();
        var response = ynResponse != null && ynResponse.Equals("y",
 StringComparison.InvariantCultureIgnoreCase);
        return response;
    }

    /// <summary>
    /// Simple check to verify a string is an email address.
    /// </summary>
    /// <param name="email">The string to verify.</param>
    /// <returns>True if a valid email.</returns>
    private static bool IsEmail(string? email)
    {
        if (string.IsNullOrEmpty(email))
            return false;
        return Regex.IsMatch(email, @"^[^@\s]+@[^@\s]+\.[^@\s]+$",
 RegexOptions.IgnoreCase);
    }
}
```

Emballage pour les opérations de service.

```
using System.Net;
using Amazon.SimpleEmailV2;
using Amazon.SimpleEmailV2.Model;
```

```
namespace Sesv2Scenario;

/// <summary>
/// Wrapper class for Amazon Simple Email Service (SES) v2 operations.
/// </summary>
public class SESv2Wrapper
{

    private readonly IAmazonSimpleEmailServiceV2 _sesClient;

    /// <summary>
    /// Constructor for the SESv2Wrapper.
    /// </summary>
    /// <param name="sesClient">The injected SES v2 client.</param>
    public SESv2Wrapper(IAmazonSimpleEmailServiceV2 sesClient)
    {
        _sesClient = sesClient;
    }

    /// <summary>
    /// Creates a contact and adds it to the specified contact list.
    /// </summary>
    /// <param name="emailAddress">The email address of the contact.</param>
    /// <param name="contactListName">The name of the contact list.</param>
    /// <returns>The response from the CreateContact operation.</returns>
    public async Task<bool> CreateContactAsync(string emailAddress, string
 contactListName)
    {
        var request = new CreateContactRequest
        {
            EmailAddress = emailAddress,
            ContactListName = contactListName
        };

        try
        {
            var response = await _sesClient.CreateContactAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (AlreadyExistsException ex)
        {
            Console.WriteLine($"Contact with email address {emailAddress} already
 exists in the contact list {contactListName}.");
            Console.WriteLine(ex.Message);
```

```
            return true;
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The contact list {contactListName} does not
exist.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while creating the contact:
{ex.Message}");
        }
        return false;
    }

    /// <summary>
    /// Creates a contact list with the specified name.
    /// </summary>
    /// <param name="contactListName">The name of the contact list.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> CreateContactListAsync(string contactListName)
    {
        var request = new CreateContactListRequest
        {
            ContactListName = contactListName
        };

        try
        {
            var response = await _sesClient.CreateContactListAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (AlreadyExistsException ex)
        {
            Console.WriteLine($"Contact list with name {contactListName} already
exists.");
            Console.WriteLine(ex.Message);
```

```
            return true;
        }
        catch (LimitExceededException ex)
        {
            Console.WriteLine("The limit for contact lists has been exceeded.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while creating the contact
list: {ex.Message}");
        }
        return false;
    }

    /// <summary>
    /// Creates an email identity (email address or domain) and starts the
verification process.
    /// </summary>
    /// <param name="emailIdentity">The email address or domain to create and
verify.</param>
    /// <returns>The response from the CreateEmailIdentity operation.</returns>
    public async Task<CreateEmailIdentityResponse>
CreateEmailIdentityAsync(string emailIdentity)
    {
        var request = new CreateEmailIdentityRequest
        {
            EmailIdentity = emailIdentity
        };

        try
        {
            var response = await _sesClient.CreateEmailIdentityAsync(request);
            return response;
        }
        catch (AlreadyExistsException ex)
        {
            Console.WriteLine($"Email identity {emailIdentity} already exists.");
```

```
            Console.WriteLine(ex.Message);
            throw;
        }
        catch (ConcurrentModificationException ex)
        {
            Console.WriteLine($"The email identity {emailIdentity} is being
modified by another operation or thread.");
            Console.WriteLine(ex.Message);
            throw;
        }
        catch (LimitExceededException ex)
        {
            Console.WriteLine("The limit for email identities has been
exceeded.");
            Console.WriteLine(ex.Message);
            throw;
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The email identity {emailIdentity} does not
exist.");
            Console.WriteLine(ex.Message);
            throw;
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
            throw;
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while creating the email
identity: {ex.Message}");
            throw;
        }
    }

    /// <summary>
    /// Creates an email template with the specified content.
    /// </summary>
    /// <param name="templateName">The name of the email template.</param>
    /// <param name="subject">The subject of the email template.</param>
```

```
    /// <param name="htmlContent">The HTML content of the email template.</param>
    /// <param name="textContent">The text content of the email template.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> CreateEmailTemplateAsync(string templateName, string
subject, string htmlContent, string textContent)
    {
        var request = new CreateEmailTemplateRequest
        {
            TemplateName = templateName,
            TemplateContent = new EmailTemplateContent
            {
                Subject = subject,
                Html = htmlContent,
                Text = textContent
            }
        };

        try
        {
            var response = await _sesClient.CreateEmailTemplateAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (AlreadyExistsException ex)
        {
            Console.WriteLine($"Email template with name {templateName} already
exists.");
            Console.WriteLine(ex.Message);
        }
        catch (LimitExceededException ex)
        {
            Console.WriteLine("The limit for email templates has been
exceeded.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while creating the email
template: {ex.Message}");
```

```
        }

        return false;
    }

    /// <summary>
    /// Deletes a contact list and all contacts within it.
    /// </summary>
    /// <param name="contactListName">The name of the contact list to delete.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> DeleteContactListAsync(string contactListName)
    {
        var request = new DeleteContactListRequest
        {
            ContactListName = contactListName
        };

        try
        {
            var response = await _sesClient.DeleteContactListAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (ConcurrentModificationException ex)
        {
            Console.WriteLine($"The contact list {contactListName} is being
 modified by another operation or thread.");
            Console.WriteLine(ex.Message);
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The contact list {contactListName} does not
 exist.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
 later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
```

```
            Console.WriteLine($"An error occurred while deleting the contact
 list: {ex.Message}");
        }

        return false;
    }

    /// <summary>
    /// Deletes an email identity (email address or domain).
    /// </summary>
    /// <param name="emailIdentity">The email address or domain to delete.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> DeleteEmailIdentityAsync(string emailIdentity)
    {
        var request = new DeleteEmailIdentityRequest
        {
            EmailIdentity = emailIdentity
        };

        try
        {
            var response = await _sesClient.DeleteEmailIdentityAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (ConcurrentModificationException ex)
        {
            Console.WriteLine($"The email identity {emailIdentity} is being
 modified by another operation or thread.");
            Console.WriteLine(ex.Message);
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The email identity {emailIdentity} does not
 exist.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
 later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
```

```
        {
            Console.WriteLine($"An error occurred while deleting the email
 identity: {ex.Message}");
        }

        return false;
    }

    /// <summary>
    /// Deletes an email template.
    /// </summary>
    /// <param name="templateName">The name of the email template to delete.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> DeleteEmailTemplateAsync(string templateName)
    {
        var request = new DeleteEmailTemplateRequest
        {
            TemplateName = templateName
        };

        try
        {
            var response = await _sesClient.DeleteEmailTemplateAsync(request);
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The email template {templateName} does not
 exist.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
 later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while deleting the email
 template: {ex.Message}");
        }
```

```
        return false;
    }

    /// <summary>
    /// Lists the contacts in the specified contact list.
    /// </summary>
    /// <param name="contactListName">The name of the contact list.</param>
    /// <returns>The list of contacts response from the ListContacts operation.</
returns>
    public async Task<List<Contact>> ListContactsAsync(string contactListName)
    {
        var request = new ListContactsRequest
        {
            ContactListName = contactListName
        };

        try
        {
            var response = await _sesClient.ListContactsAsync(request);
            return response.Contacts;
        }
        catch (NotFoundException ex)
        {
            Console.WriteLine($"The contact list {contactListName} does not
 exist.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
 later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while listing the contacts:
 {ex.Message}");
        }

        return new List<Contact>();
    }

    /// <summary>
    /// Sends an email with the specified content and options.
```

```
    /// </summary>
    /// <param name="fromEmailAddress">The email address to send the email
from.</param>
    /// <param name="toEmailAddresses">The email addresses to send the email
to.</param>
    /// <param name="subject">The subject of the email.</param>
    /// <param name="htmlContent">The HTML content of the email.</param>
    /// <param name="textContent">The text content of the email.</param>
    /// <param name="templateName">The name of the email template to use
(optional).</param>
    /// <param name="templateData">The data to replace placeholders in the email
template (optional).</param>
    /// <param name="contactListName">The name of the contact list for
unsubscribe functionality (optional).</param>
    /// <returns>The MessageId response from the SendEmail operation.</returns>
    public async Task<string> SendEmailAsync(string fromEmailAddress,
List<string> toEmailAddresses, string? subject,
        string? htmlContent, string? textContent, string? templateName = null,
string? templateData = null, string? contactListName = null)
    {
        var request = new SendEmailRequest
        {
            FromEmailAddress = fromEmailAddress
        };

        if (toEmailAddresses.Any())
        {
            request.Destination = new Destination { ToAddresses =
toEmailAddresses };
        }

        if (!string.IsNullOrEmpty(templateName))
        {
            request.Content = new EmailContent()
            {
                Template = new Template
                {
                    TemplateName = templateName,
                    TemplateData = templateData
                }
            };
        }
        else
        {
```

```
            request.Content = new EmailContent
            {
                Simple = new Message
                {
                    Subject = new Content { Data = subject },
                    Body = new Body
                    {
                        Html = new Content { Data = htmlContent },
                        Text = new Content { Data = textContent }
                    }
                }
            };
        }

        if (!string.IsNullOrEmpty(contactListName))
        {
            request.ListManagementOptions = new ListManagementOptions
            {
                ContactListName = contactListName
            };
        }

        try
        {
            var response = await _sesClient.SendEmailAsync(request);
            return response.MessageId;
        }
        catch (AccountSuspendedException ex)
        {
            Console.WriteLine("The account's ability to send email has been
permanently restricted.");
            Console.WriteLine(ex.Message);
        }
        catch (MailFromDomainNotVerifiedException ex)
        {
            Console.WriteLine("The sending domain is not verified.");
            Console.WriteLine(ex.Message);
        }
        catch (MessageRejectedException ex)
        {
            Console.WriteLine("The message content is invalid.");
            Console.WriteLine(ex.Message);
        }
        catch (SendingPausedException ex)
```

```
        {
            Console.WriteLine("The account's ability to send email is currently
 paused.");
            Console.WriteLine(ex.Message);
        }
        catch (TooManyRequestsException ex)
        {
            Console.WriteLine("Too many requests were made. Please try again
 later.");
            Console.WriteLine(ex.Message);
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred while sending the email:
 {ex.Message}");
        }

        return string.Empty;
    }
}
```

- Pour plus d'informations sur l'API consultez les rubriques suivantes dans la référence de l'API AWS SDK for .NET .
  - CreateContact
  - CreateContactList
  - CreateEmailIdentity
  - CreateEmailTemplate
  - DeleteContactList
  - DeleteEmailIdentity
  - DeleteEmailTemplate
  - ListContacts
  - SendEmail.simple
  - SendEmail.modèle

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    try {
      // 2. Create a contact list
      String contactListName = CONTACT_LIST_NAME;
      CreateContactListRequest createContactListRequest =
 CreateContactListRequest.builder()
          .contactListName(contactListName)
          .build();
      sesClient.createContactList(createContactListRequest);
      System.out.println("Contact list created: " + contactListName);
    } catch (AlreadyExistsException e) {
      System.out.println("Contact list already exists, skipping creation: weekly-
coupons-newsletter");
    } catch (LimitExceededException e) {
      System.err.println("Limit for contact lists has been exceeded.");
      throw e;
    } catch (SesV2Exception e) {
      System.err.println("Error creating contact list: " + e.getMessage());
      throw e;
    }

      try {
        // Create a new contact with the provided email address in the
        CreateContactRequest contactRequest = CreateContactRequest.builder()
            .contactListName(CONTACT_LIST_NAME)
            .emailAddress(emailAddress)
            .build();

        sesClient.createContact(contactRequest);
        contacts.add(emailAddress);

        System.out.println("Contact created: " + emailAddress);
```

```
        // Send a welcome email to the new contact
        String welcomeHtml = Files.readString(Paths.get("resources/
coupon_newsletter/welcome.html"));
        String welcomeText = Files.readString(Paths.get("resources/
coupon_newsletter/welcome.txt"));

        SendEmailRequest welcomeEmailRequest = SendEmailRequest.builder()
            .fromEmailAddress(this.verifiedEmail)
            .destination(Destination.builder().toAddresses(emailAddress).build())
            .content(EmailContent.builder()
                .simple(
                    Message.builder()
                        .subject(Content.builder().data("Welcome to the Weekly
 Coupons Newsletter").build())
                        .body(Body.builder()
                            .text(Content.builder().data(welcomeText).build())
                            .html(Content.builder().data(welcomeHtml).build())
                            .build())
                        .build())
                .build())
            .build();
        SendEmailResponse welcomeEmailResponse =
 sesClient.sendEmail(welcomeEmailRequest);
        System.out.println("Welcome email sent: " +
 welcomeEmailResponse.messageId());
      } catch (AlreadyExistsException e) {
        // If the contact already exists, skip this step for that contact and
 proceed
        // with the next contact
        System.out.println("Contact already exists, skipping creation...");
      } catch (Exception e) {
        System.err.println("Error occurred while processing email address " +
 emailAddress + ": " + e.getMessage());
        throw e;
      }
    }

      ListContactsRequest contactListRequest = ListContactsRequest.builder()
          .contactListName(CONTACT_LIST_NAME)
          .build();

      List<String> contactEmails;
      try {
```

```
        ListContactsResponse contactListResponse =
 sesClient.listContacts(contactListRequest);

        contactEmails = contactListResponse.contacts().stream()
            .map(Contact::emailAddress)
            .toList();
      } catch (Exception e) {
        // TODO: Remove when listContacts's GET body issue is resolved.
        contactEmails = this.contacts;
      }


      String coupons = Files.readString(Paths.get("resources/coupon_newsletter/
sample_coupons.json"));
      for (String emailAddress : contactEmails) {
        SendEmailRequest newsletterRequest = SendEmailRequest.builder()
            .destination(Destination.builder().toAddresses(emailAddress).build())
            .content(EmailContent.builder()
                .template(Template.builder()
                    .templateName(TEMPLATE_NAME)
                    .templateData(coupons)
                    .build())
                .build())
            .fromEmailAddress(this.verifiedEmail)
            .listManagementOptions(ListManagementOptions.builder()
                .contactListName(CONTACT_LIST_NAME)
                .build())
            .build();
        SendEmailResponse newsletterResponse =
 sesClient.sendEmail(newsletterRequest);
        System.out.println("Newsletter sent to " + emailAddress + ": " +
 newsletterResponse.messageId());
      }

    try {
      CreateEmailIdentityRequest createEmailIdentityRequest =
 CreateEmailIdentityRequest.builder()
          .emailIdentity(verifiedEmail)
          .build();
      sesClient.createEmailIdentity(createEmailIdentityRequest);
      System.out.println("Email identity created: " + verifiedEmail);
    } catch (AlreadyExistsException e) {
      System.out.println("Email identity already exists, skipping creation: " +
 verifiedEmail);
```

```
    } catch (NotFoundException e) {
      System.err.println("The provided email address is not verified: " +
 verifiedEmail);
      throw e;
    } catch (LimitExceededException e) {
      System.err
          .println("You have reached the limit for email identities. Please
 remove some identities and try again.");
      throw e;
    } catch (SesV2Exception e) {
      System.err.println("Error creating email identity: " + e.getMessage());
      throw e;
    }

    try {
      // Create an email template named "weekly-coupons"
      String newsletterHtml = loadFile("resources/coupon_newsletter/coupon-
newsletter.html");
      String newsletterText = loadFile("resources/coupon_newsletter/coupon-
newsletter.txt");

      CreateEmailTemplateRequest templateRequest =
 CreateEmailTemplateRequest.builder()
          .templateName(TEMPLATE_NAME)
          .templateContent(EmailTemplateContent.builder()
              .subject("Weekly Coupons Newsletter")
              .html(newsletterHtml)
              .text(newsletterText)
              .build())
          .build();

      sesClient.createEmailTemplate(templateRequest);

      System.out.println("Email template created: " + TEMPLATE_NAME);
    } catch (AlreadyExistsException e) {
      // If the template already exists, skip this step and proceed with the next
      // operation
      System.out.println("Email template already exists, skipping creation...");
    } catch (LimitExceededException e) {
      // If the limit for email templates is exceeded, fail the workflow and
 inform
      // the user
      System.err.println("You have reached the limit for email templates. Please
 remove some templates and try again.");
```

```
            throw e;
        } catch (Exception e) {
            System.err.println("Error occurred while creating email template: " +
e.getMessage());
            throw e;
        }

        try {
            // Delete the contact list
            DeleteContactListRequest deleteContactListRequest =
DeleteContactListRequest.builder()
                    .contactListName(CONTACT_LIST_NAME)
                    .build();

            sesClient.deleteContactList(deleteContactListRequest);

            System.out.println("Contact list deleted: " + CONTACT_LIST_NAME);
        } catch (NotFoundException e) {
            // If the contact list does not exist, log the error and proceed
            System.out.println("Contact list not found. Skipping deletion...");
        } catch (Exception e) {
            System.err.println("Error occurred while deleting the contact list: " +
e.getMessage());
            e.printStackTrace();
        }

            try {
              // Delete the email identity
              DeleteEmailIdentityRequest deleteIdentityRequest =
DeleteEmailIdentityRequest.builder()
                      .emailIdentity(this.verifiedEmail)
                      .build();

              sesClient.deleteEmailIdentity(deleteIdentityRequest);

              System.out.println("Email identity deleted: " + this.verifiedEmail);
            } catch (NotFoundException e) {
              // If the email identity does not exist, log the error and proceed
              System.out.println("Email identity not found. Skipping deletion...");
            } catch (Exception e) {
              System.err.println("Error occurred while deleting the email identity: " +
e.getMessage());
              e.printStackTrace();
            }
```

```
    } else {
      System.out.println("Skipping email identity deletion.");
    }

    try {
      // Delete the template
      DeleteEmailTemplateRequest deleteTemplateRequest =
DeleteEmailTemplateRequest.builder()
          .templateName(TEMPLATE_NAME)
          .build();

      sesClient.deleteEmailTemplate(deleteTemplateRequest);

      System.out.println("Email template deleted: " + TEMPLATE_NAME);
    } catch (NotFoundException e) {
      // If the email template does not exist, log the error and proceed
      System.out.println("Email template not found. Skipping deletion...");
    } catch (Exception e) {
      System.err.println("Error occurred while deleting the email template: " +
e.getMessage());
      e.printStackTrace();
    }
```

- Pour plus d'informations sur l'API, consultez les rubriques suivantes dans la référence de l'API AWS SDK for Java 2.x .
  - CreateContact
  - CreateContactList
  - CreateEmailIdentity
  - CreateEmailTemplate
  - DeleteContactList
  - DeleteEmailIdentity
  - DeleteEmailTemplate
  - ListContacts
  - SendEmail.simple
  - SendEmail.modèle

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


        try:

 self.ses_client.create_contact_list(ContactListName=CONTACT_LIST_NAME)
            print(f"Contact list '{CONTACT_LIST_NAME}' created successfully.")
```

```
        except ClientError as e:
            # If the contact list already exists, skip and proceed
            if e.response["Error"]["Code"] == "AlreadyExistsException":
                print(f"Contact list '{CONTACT_LIST_NAME}' already exists.")
            else:
                raise e

            try:
                # Create a new contact
                self.ses_client.create_contact(
                    ContactListName=CONTACT_LIST_NAME, EmailAddress=email
                )
                print(f"Contact with email '{email}' created successfully.")

                # Send the welcome email
                self.ses_client.send_email(
                    FromEmailAddress=self.verified_email,
                    Destination={"ToAddresses": [email]},
                    Content={
                        "Simple": {
                            "Subject": {
                                "Data": "Welcome to the Weekly Coupons
Newsletter"
                            },
                            "Body": {
                                "Text": {"Data": welcome_text},
                                "Html": {"Data": welcome_html},
                            },
                        }
                    },
                )
                print(f"Welcome email sent to '{email}'.")
                if self.sleep:
                    # 1 email per second in sandbox mode, remove in production.
                    sleep(1.1)
            except ClientError as e:
                # If the contact already exists, skip and proceed
                if e.response["Error"]["Code"] == "AlreadyExistsException":
                    print(f"Contact with email '{email}' already exists.
Skipping...")
                else:
                    raise e

        try:
```

```
            contacts_response = self.ses_client.list_contacts(
                ContactListName=CONTACT_LIST_NAME
            )
        except ClientError as e:
            if e.response["Error"]["Code"] == "NotFoundException":
                print(f"Contact list '{CONTACT_LIST_NAME}' does not exist.")
                return
            else:
                raise e

                self.ses_client.send_email(
                    FromEmailAddress=self.verified_email,
                    Destination={"ToAddresses": [email]},
                    Content={
                        "Simple": {
                            "Subject": {
                                "Data": "Welcome to the Weekly Coupons
Newsletter"
                            },
                            "Body": {
                                "Text": {"Data": welcome_text},
                                "Html": {"Data": welcome_html},
                            },
                        }
                    },
                )
                print(f"Welcome email sent to '{email}'.")

                self.ses_client.send_email(
                    FromEmailAddress=self.verified_email,
                    Destination={"ToAddresses": [email_address]},
                    Content={
                        "Template": {
                            "TemplateName": TEMPLATE_NAME,
                            "TemplateData": coupon_items,
                        }
                    },
                    ListManagementOptions={"ContactListName": CONTACT_LIST_NAME},
                )

        try:

self.ses_client.create_email_identity(EmailIdentity=self.verified_email)
```

```
            print(f"Email identity '{self.verified_email}' created
successfully.")
        except ClientError as e:
            # If the email identity already exists, skip and proceed
            if e.response["Error"]["Code"] == "AlreadyExistsException":
                print(f"Email identity '{self.verified_email}' already exists.")
            else:
                raise e

        try:
            template_content = {
                "Subject": "Weekly Coupons Newsletter",
                "Html": load_file_content("coupon-newsletter.html"),
                "Text": load_file_content("coupon-newsletter.txt"),
            }
            self.ses_client.create_email_template(
                TemplateName=TEMPLATE_NAME, TemplateContent=template_content
            )
            print(f"Email template '{TEMPLATE_NAME}' created successfully.")
        except ClientError as e:
            # If the template already exists, skip and proceed
            if e.response["Error"]["Code"] == "AlreadyExistsException":
                print(f"Email template '{TEMPLATE_NAME}' already exists.")
            else:
                raise e

        try:

self.ses_client.delete_contact_list(ContactListName=CONTACT_LIST_NAME)
            print(f"Contact list '{CONTACT_LIST_NAME}' deleted successfully.")
        except ClientError as e:
            # If the contact list doesn't exist, skip and proceed
            if e.response["Error"]["Code"] == "NotFoundException":
                print(f"Contact list '{CONTACT_LIST_NAME}' does not exist.")
            else:
                print(e)

            try:

self.ses_client.delete_email_identity(EmailIdentity=self.verified_email)
                print(f"Email identity '{self.verified_email}' deleted
successfully.")
            except ClientError as e:
                # If the email identity doesn't exist, skip and proceed
```

```
                if e.response["Error"]["Code"] == "NotFoundException":
                    print(f"Email identity '{self.verified_email}' does not
exist.")
                else:
                    print(e)

        try:
            self.ses_client.delete_email_template(TemplateName=TEMPLATE_NAME)
            print(f"Email template '{TEMPLATE_NAME}' deleted successfully.")
        except ClientError as e:
            # If the email template doesn't exist, skip and proceed
            if e.response["Error"]["Code"] == "NotFoundException":
                print(f"Email template '{TEMPLATE_NAME}' does not exist.")
            else:
                print(e)
```

- Pour plus d'informations sur l'API, consultez les rubriques suivantes dans AWS SDK for Python (Boto3) API Reference.
  - CreateContact
  - CreateContactList
  - CreateEmailIdentity
  - CreateEmailTemplate
  - DeleteContactList
  - DeleteEmailIdentity
  - DeleteEmailTemplate
  - ListContacts
  - SendEmail.simple
  - SendEmail.modèle

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus sur GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
        match self
            .client
            .create_contact_list()
            .contact_list_name(CONTACT_LIST_NAME)
            .send()
            .await
        {
            Ok(_) => writeln!(self.stdout, "Contact list created
successfully.")?,
            Err(e) => match e.into_service_error() {
                CreateContactListError::AlreadyExistsException(_) => {
                    writeln!(
                        self.stdout,
                        "Contact list already exists, skipping creation."
                    )?;
                }
                e => return Err(anyhow!("Error creating contact list: {}", e)),
            },
        }

            match self
                .client
                .create_contact()
                .contact_list_name(CONTACT_LIST_NAME)
                .email_address(email.clone())
                .send()
                .await
            {
                Ok(_) => writeln!(self.stdout, "Contact created for {}", email)?,
                Err(e) => match e.into_service_error() {
                    CreateContactError::AlreadyExistsException(_) => writeln!(
                        self.stdout,
```

```
                        "Contact already exists for {}, skipping creation.",
                        email
                    )?,
                    e => return Err(anyhow!("Error creating contact for {}: {}",
 email, e)),
                },
            }

        let contacts: Vec<Contact> = match self
            .client
            .list_contacts()
            .contact_list_name(CONTACT_LIST_NAME)
            .send()
            .await
        {
            Ok(list_contacts_output) => {
                list_contacts_output.contacts.unwrap().into_iter().collect()
            }
            Err(e) => {
                return Err(anyhow!(
                    "Error retrieving contact list {}: {}",
                    CONTACT_LIST_NAME,
                    e
                ))
            }
        };

            let coupons = std::fs::read_to_string("../resources/newsletter/
sample_coupons.json")
                .unwrap_or_else(|_| r#"{"coupons":[]}"#.to_string());
            let email_content = EmailContent::builder()
                .template(
                    Template::builder()
                        .template_name(TEMPLATE_NAME)
                        .template_data(coupons)
                        .build(),
                )
                .build();

            match self
                .client
                .send_email()
                .from_email_address(self.verified_email.clone())
```

```
.destination(Destination::builder().to_addresses(email.clone()).build())
                .content(email_content)
                .list_management_options(
                    ListManagementOptions::builder()
                        .contact_list_name(CONTACT_LIST_NAME)
                        .build()?,
                )
                .send()
                .await
            {
                Ok(output) => {
                    if let Some(message_id) = output.message_id {
                        writeln!(
                            self.stdout,
                            "Newsletter sent to {} with message ID {}",
                            email, message_id
                        )?;
                    } else {
                        writeln!(self.stdout, "Newsletter sent to {}", email)?;
                    }
                }
                Err(e) => return Err(anyhow!("Error sending newsletter to {}:
{}", email, e)),
            }

        match self
            .client
            .create_email_identity()
            .email_identity(self.verified_email.clone())
            .send()
            .await
        {
            Ok(_) => writeln!(self.stdout, "Email identity created
successfully.")?,
            Err(e) => match e.into_service_error() {
                CreateEmailIdentityError::AlreadyExistsException(_) => {
                    writeln!(
                        self.stdout,
                        "Email identity already exists, skipping creation."
                    )?;
                }
                e => return Err(anyhow!("Error creating email identity: {}", e)),
            },
```

```
        }

        let template_html =
            std::fs::read_to_string("../resources/newsletter/coupon-
newsletter.html")
                .unwrap_or_else(|_| "Missing coupon-
newsletter.html".to_string());
        let template_text =
            std::fs::read_to_string("../resources/newsletter/coupon-
newsletter.txt")
                .unwrap_or_else(|_| "Missing coupon-newsletter.txt".to_string());

        // Create the email template
        let template_content = EmailTemplateContent::builder()
            .subject("Weekly Coupons Newsletter")
            .html(template_html)
            .text(template_text)
            .build();

        match self
            .client
            .create_email_template()
            .template_name(TEMPLATE_NAME)
            .template_content(template_content)
            .send()
            .await
        {
            Ok(_) => writeln!(self.stdout, "Email template created
 successfully.")?,
            Err(e) => match e.into_service_error() {
                CreateEmailTemplateError::AlreadyExistsException(_) => {
                    writeln!(
                        self.stdout,
                        "Email template already exists, skipping creation."
                    )?;
                }
                e => return Err(anyhow!("Error creating email template: {}", e)),
            },
        }

        match self
            .client
            .delete_contact_list()
            .contact_list_name(CONTACT_LIST_NAME)
```

```
            .send()
            .await
        {
            Ok(_) => writeln!(self.stdout, "Contact list deleted
successfully.")?,
            Err(e) => return Err(anyhow!("Error deleting contact list: {e}")),
        }

            match self
                .client
                .delete_email_identity()
                .email_identity(self.verified_email.clone())
                .send()
                .await
            {
                Ok(_) => writeln!(self.stdout, "Email identity deleted
successfully.")?,
                Err(e) => {
                    return Err(anyhow!("Error deleting email identity: {}", e));
                }
            }

        match self
            .client
            .delete_email_template()
            .template_name(TEMPLATE_NAME)
            .send()
            .await
        {
            Ok(_) => writeln!(self.stdout, "Email template deleted
successfully.")?,
            Err(e) => {
                return Err(anyhow!("Error deleting email template: {e}"));
            }
        }
```

- Pour plus d'informations sur l'API, consultez les rubriques suivantes dans AWS SDK for Rust API reference.
  - CreateContact
  - CreateContactList
  - CreateEmailIdentity

- CreateEmailTemplate
- DeleteContactList
- DeleteEmailIdentity
- DeleteEmailTemplate
- ListContacts
- SendEmail.simple
- SendEmail.modèle

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation d'Amazon SES avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Sécurité dans Amazon Simple Email Service

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon Simple Email Service, consultez les AWS sections Services concernés par programme AWS de conformité et .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise et la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'Amazon Simple Email Service. Elle vous montre comment configurer Amazon Simple Email Service pour atteindre vos objectifs en matière de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser les ressources de votre Amazon Simple Email Service.

> **Note**
>
> Si vous devez signaler un abus de AWS ressources, notamment du spam par e-mail et la distribution de logiciels malveillants, n'utilisez le lien de commentaires figurant sur aucune des pages de ce guide du développeur, car le formulaire est reçu par l'équipe de AWS documentation, et non par AWS Trust & Safety. Au lieu de cela, sur la page Comment signaler un abus de AWS ressources ? page, suivez les instructions pour contacter l'équipe AWS Trust & Safety afin de signaler tout type d' AWS abus sur Amazon.

Table des matières

Protection des données dans Amazon Simple Email Service

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans Amazon Simple Email Service. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.

- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Amazon Simple Email Service ou un autre service à Services AWS l'aide de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Table des matières

Chiffrement des données au repos pour Amazon SES

Par défaut, Amazon SES chiffre toutes les données au repos. Le chiffrement par défaut permet de réduire les frais opérationnels et la complexité liés à la protection des données. Le chiffrement vous permet également de créer des archives Mail Manager qui répondent aux exigences réglementaires et de conformité strictes en matière de chiffrement.

SES propose les options de chiffrement suivantes :

- AWS clés détenues : SES les utilise par défaut. Vous ne pouvez pas afficher, gérer ou utiliser les clés que vous AWS possédez, ni auditer leur utilisation. Toutefois, vous n'avez pas besoin de prendre de mesure ou de modifier les programmes pour protéger les clés qui chiffrent vos données. Pour plus d'informations, consultez Clés détenues par AWS dans le Guide du développeur AWS Key Management Service .

- Clés gérées par le client : SES prend en charge l'utilisation de clés symétriques gérées par le client que vous créez, détenez et gérez. Comme vous avez le contrôle total du chiffrement, vous pouvez effectuer des tâches telles que :
  - Établissement et gestion des stratégies de clé
  - Établissement et gestion des politiques IAM et des octrois
  - Activation et désactivation des stratégies de clé
  - Rotation des matériaux de chiffrement de clé
  - Ajout de balises
  - Création d'alias de clé
  - Planification des clés pour la suppression

  Pour utiliser votre propre clé, choisissez une clé gérée par le client lorsque vous créez vos ressources SES.

  Pour plus d'informations, consultez Clés gérées par le client dans le Guide du développeur AWS Key Management Service (langue française non garantie).

> **Note**
>
> SES active automatiquement le chiffrement au repos à l'aide de clés AWS détenues gratuitement.
> Toutefois, AWS KMS des frais s'appliquent pour l'utilisation d'une clé gérée par le client. Pour plus d'informations sur les tarifs, consultez les AWS Key Management Service tarifs.

Création d’une clé gérée par le client

Vous pouvez créer une clé symétrique gérée par le client à l'aide de AWS Management Console, ou des AWS KMS API.

Pour créer une clé symétrique gérée par le client

Suivez les étapes de création de clés KMS de chiffrement symétriques décrites dans le manuel du AWS Key Management Service développeur.

> **Note**
>
> Pour l'archivage, votre clé doit répondre aux exigences suivantes :
>
> - La clé doit être symétrique.
> - L'origine du matériau clé doit êtreAWS_KMS.
> - La clé d'utilisation doit êtreENCRYPT_DECRYPT.

Stratégie de clé

Les politiques de clés contrôlent l'accès à votre clé gérée par le client. Chaque clé gérée par le client doit avoir exactement une stratégie de clé, qui contient des instructions qui déterminent les personnes pouvant utiliser la clé et comment elles peuvent l'utiliser. Lorsque vous créez votre clé gérée par le client, vous pouvez spécifier une stratégie de clé. Pour plus d'informations, consultez Gestion de l'accès aux clés gérées par le client dans le Guide du développeur AWS Key Management Service .

Pour utiliser votre clé gérée par le client dans le cadre de l'archivage de Mail Manager, votre politique en matière de clés doit autoriser les opérations d'API suivantes :

- kms : DescribeKey — Fournit les informations relatives aux clés gérées par le client qui permettent à SES de valider la clé.
- kms : GenerateDataKey — Permet à SES de générer une clé de données pour chiffrer les données au repos.
- KMS:Decrypt — Permet à SES de déchiffrer les données stockées avant de les renvoyer aux clients de l'API.

L'exemple suivant illustre une politique clé typique :

```
{
            "Sid": "Allow SES to encrypt/decrypt",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
```

```
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
```

Pour plus d'informations, consultez la section Spécification des autorisations dans une politique, dans le Guide du AWS Key Management Service développeur.

Pour plus d'informations sur le dépannage, consultez la section Résolution des problèmes d'accès par clé dans le Guide du AWS Key Management Service développeur.

Spécification d'une clé gérée par le client pour l'archivage de Mail Manager

Vous pouvez spécifier une clé gérée par le client au lieu d'utiliser des clés AWS détenues. Lorsque vous créez une archive, vous pouvez spécifier la clé de données en saisissant un ARN de clé KMS, que Mail Manager Archiving utilise pour chiffrer toutes les données client de l'archive.

- ARN de la clé KMS : identifiant de clé pour une clé gérée par le AWS KMS client. Saisissez un ID de clé, un ARN de clé, un nom d'alias ou un ARN d'alias.

Contexte du chiffrement Amazon SES

Un contexte de chiffrement est un ensemble facultatif de paires clé-valeur qui contient des informations contextuelles supplémentaires sur les données.

AWS KMS utilise le contexte de chiffrement comme données authentifiées supplémentaires pour prendre en charge le chiffrement authentifié. Lorsque vous incluez un contexte de chiffrement dans une demande de chiffrement de données, AWS KMS lie le contexte de chiffrement aux données chiffrées. Pour déchiffrer les données, vous devez inclure le même contexte de chiffrement dans la demande.

> **Note**
>
> Amazon SES ne prend pas en charge les contextes de chiffrement pour la création d'archives. Vous utilisez plutôt une politique IAM ou KMS. Pour des exemples de politiquesPolitiques de création d'archives, voir plus loin dans cette section.

Contexte de chiffrement Amazon SES

SES utilise le même contexte de chiffrement dans toutes les opérations AWS KMS cryptographiques, où la clé `aws:ses:arn` et la valeur sont la ressource Amazon Resource Name (ARN).

Example

```
"encryptionContext": {
    "aws:ses:arn": "arn:aws:ses:us-west-2:111122223333:ExampleResourceName/
ExampleResourceID"
}
```

Utilisation du contexte de chiffrement pour la surveillance

Lorsque vous utilisez une clé symétrique gérée par le client pour chiffrer votre ressource SES, vous pouvez également utiliser le contexte de chiffrement dans les enregistrements et les journaux d'audit pour identifier la manière dont la clé gérée par le client est utilisée. Le contexte de chiffrement apparaît également dans les journaux générés par AWS CloudTrail ou Amazon CloudWatch Logs.

Utilisation du contexte de chiffrement pour contrôler l'accès à votre clé gérée par le client

Vous pouvez utiliser le contexte de chiffrement dans les stratégies de clé et les politiques IAM comme `conditions` pour contrôler l'accès à votre clé symétrique gérée par le client. Vous pouvez également utiliser des contraintes de contexte de chiffrement dans un octroi.

SES utilise une contrainte de contexte de chiffrement dans les autorisations afin de contrôler l'accès à la clé gérée par le client dans votre compte ou votre région. La contrainte d'octroi exige que les opérations autorisées par l'octroi utilisent le contexte de chiffrement spécifié.

Example

Vous trouverez ci-dessous des exemples de déclarations de stratégie de clé permettant d'accorder l'accès à une clé gérée par le client dans un contexte de chiffrement spécifique. La condition énoncée dans cette déclaration de stratégie exige que les octrois comportent une contrainte de contexte de chiffrement qui spécifie le contexte de chiffrement.

```
{
    "Sid": "Enable DescribeKey",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
     },
```

```
     "Action": "kms:DescribeKey",
     "Resource": "*"
},
{
     "Sid": "Enable CreateGrant",
     "Effect": "Allow",
     "Principal": {
         "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
     },
     "Action": "kms:CreateGrant",
     "Resource": "*",
     "Condition": {
         "StringEquals": {
             "kms:EncryptionContext:aws:ses:arn": "arn:aws:ses:us-
west-2:111122223333:ExampleResourceName/ExampleResourceID"
          }
     }
}
```

Politiques de création d'archives

Les exemples de politiques suivants montrent comment activer la création d'archives. Les politiques s'appliquent à tous les actifs.

Politique IAM

```
{
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ses:CreateArchive",
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*",
            "Condition": {
```

```
                "StringEquals": {
                    "kms:ViaService": "ses.us-east-1.amazonaws.com",
                    "kms:CallerAccount": "012345678910"
                }
            }
        }
```

AWS KMS stratégie

```
{
            "Sid": "Allow SES to encrypt/decrypt",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
```

Surveillance de vos clés de chiffrement pour Amazon SES

Lorsque vous utilisez une clé gérée par le AWS KMS client avec vos ressources Amazon SES, vous pouvez utiliser AWS CloudTrailAmazon CloudWatch Logs pour suivre les demandes auxquelles SES envoie AWS KMS.

Les exemples suivants sont AWS CloudTrail des événements destinés à `GenerateDataKeyDecrypt`, et `DescribeKey` pour surveiller les opérations KMS appelées par SES pour accéder aux données chiffrées par votre clé gérée par le client :

GenerateDataKey

Lorsque vous activez une clé gérée par le AWS KMS client pour votre ressource, SES crée une clé de table unique. Il envoie une `GenerateDataKey` demande AWS KMS qui spécifie la clé gérée par le AWS KMS client pour la ressource.

Lorsque vous activez une clé gérée par le AWS KMS client pour votre ressource d'archive Mail Manager, elle est utilisée `GenerateDataKey` pour chiffrer les données d'archive au repos.

L'exemple d'événement suivant enregistre l'opération `GenerateDataKey` :


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "ses.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "encryptionContext": {
            "aws:ses:arn": "arn:aws:ses:us-west-2:111122223333:ExampleResourceName/
ExampleResourceID"
        },
        "keySpec": "AES_256",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333",
    "sharedEventID": "57f5dbee-16da-413e-979f-2c4c6663475e"
}
```

Decrypt

Lorsque vous accédez à une ressource cryptée, SES appelle l'`Decrypt`opération pour utiliser la clé de données cryptée stockée afin d'accéder aux données cryptées.

L'exemple d'événement suivant enregistre l'opération `Decrypt` :


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "ses.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:10:51Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "encryptionContext": {
            "aws:ses:arn": "arn:aws:ses:us-west-2:111122223333:ExampleResourceName/
ExampleResourceID"
        },
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333",
```

```
    "sharedEventID": "dc129381-1d94-49bd-b522-f56a3482d088"
}
```

DescribeKey

SES utilise cette `DescribeKey` opération pour vérifier si la clé gérée par le AWS KMS client associée à votre ressource existe dans le compte et dans la région.

L'exemple d'événement suivant enregistre l'opération `DescribeKey` :

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-04-22T17:02:00Z"
            }
        },
        "invokedBy": "ses.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "keyId": "00dd0db0-0000-0000-ac00-b0c000SAMPLE"
    },
    "responseElements": null,
```

```
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```


En savoir plus

Les ressources suivantes fournissent plus d'informations sur le chiffrement des données au repos.

- Pour plus d'informations sur les concepts de base AWS Key Management Service, consultez le Guide du développeur AWS Key Management Service .
- Pour plus d'informations sur les Bonnes pratiques de sécurité pour AWS Key Management Service, consultez le Guide du développeur AWS Key Management Service .

Chiffrement en transit

Par défaut, Amazon SES utilise la méthode TLS opportuniste. Cela signifie qu'Amazon SES tente toujours de créer une connexion sécurisée au serveur de messagerie de réception. S'il ne peut pas établir une connexion sécurisée, il envoie le message non chiffré. Vous pouvez modifier ce comportement de sorte qu'Amazon SES envoie le message au serveur de messagerie de réception uniquement s'il peut établir une connexion sécurisée. Pour plus d'informations, voir Amazon SES et protocoles de sécurité.

Suppression de données personnelles d'Amazon SES

En fonction de la façon dont vous l'utilisez, Amazon SES peut stocker certaines données pouvant être considérées comme des renseignements personnels. Par exemple, pour envoyer des e-mails

à l'aide d'Amazon SES, vous devez fournir au moins une identité vérifiée (une adresse e-mail ou un domaine). Vous pouvez utiliser la console Amazon SES ou l'API Amazon SES pour supprimer définitivement ces données personnelles.

Ce chapitre indique des procédures pour supprimer différents types de données pouvant être considérées comme des renseignements personnels.

Table des matières

Supprimer les adresses e-mail de la liste de suppression au niveau du compte

Amazon SES inclut une liste optionnelle de suppression au niveau du compte. Lorsque vous activez cette fonctionnalité, les adresses e-mail sont automatiquement ajoutées à une liste de suppression lorsqu'elles entraînent un retour à l'expéditeur ou une réclamation. Les adresses e-mail figurent dans cette liste jusqu'à ce que vous les supprimiez. Pour en savoir plus sur la liste de suppression au niveau du compte, veuillez consulter Utilisation de la liste de suppression au niveau du compte Amazon SES.

Vous pouvez supprimer des adresses e-mail de la liste de suppression au niveau du compte en utilisant l'opération `DeleteSuppressedDestination` dans l'API v2 Amazon SES. Cette section comprend une procédure de suppression des adresses e-mail à l'aide de l' AWS CLI. Pour en savoir plus sur l'installation et la configuration de l' AWS CLI, consultez le Guide de l'utilisateur de l'AWS Command Line Interface.

Pour supprimer une adresse de la liste de suppression au niveau du compte à l'aide de l' AWS CLI

- Sur la ligne de commande, entrez la commande suivante :

```
aws sesv2 delete-suppressed-destination --email-address recipient@example.com
```

Dans la commande précédente, remplacez *recipient@example.com* par l'adresse e-mail que vous souhaitez supprimer de la liste de suppression au niveau du compte.

Supprimer des données relatives à des e-mails envoyés à l'aide d'Amazon SES

Lorsque vous utilisez Amazon SES pour envoyer un e-mail, vous pouvez envoyer des informations concernant cet e-mail à d'autres AWS services. Par exemple, vous pouvez envoyer des informations sur les événements liés aux e-mails (tels que les livraisons, les ouvertures et les clics) à Firehose. Ces données d'événement contiennent généralement votre adresse e-mail et de l'adresse IP à partir de laquelle l'e-mail a été envoyé. Elles contient également les adresses électroniques de tous les destinataires de l'e-mail.

Vous pouvez utiliser Firehose pour diffuser les données d'événements par e-mail vers plusieurs destinations, notamment Amazon Simple Storage Service, Amazon Service et OpenSearch Amazon Redshift. Pour supprimer ces données, vous devez d'abord arrêter de diffuser des données vers Firehose, puis supprimer les données déjà diffusées. Pour arrêter de diffuser les données d'événements Amazon SES vers Firehose, vous devez supprimer la destination de l'événement Firehose.

Pour supprimer la destination d'un événement Firehose à l'aide de la console Amazon SES

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/ses/.
2. Sous Email Sending (Envoi d'e-mails), choisissez Configuration Sets (Jeux de configurations).
3. Dans la liste des ensembles de configuration, choisissez le jeu de configuration qui contient la destination de l'événement Firehose.
4. À côté de la destination de l'événement Firehose que vous souhaitez supprimer, cliquez sur le bouton delete
   ( ).
5. Si nécessaire, supprimez les données que Firehose a écrites à d'autres services. Pour de plus amples informations, veuillez consulter the section called “Supprimer les données d'événement stockées”.

Vous pouvez également utiliser l'API Amazon SES pour supprimer des destinations d'événements. La procédure suivante utilise le AWS Command Line Interface (AWS CLI) pour interagir avec l'API Amazon SES. Vous pouvez également interagir avec l'API à l'aide d'un AWS SDK ou en effectuant directement des requêtes HTTP.

Pour supprimer la destination d'un événement Firehose à l'aide du AWS CLI

1. Sur la ligne de commande, entrez la commande suivante :

   ```
   aws sesv2 delete-configuration-set-event-destination --configuration-set-
   name configSet \
   --event-destination-name eventDestination
   ```

   Dans cette commande, remplacez *ConfigSet* par le nom du jeu de configuration contenant la destination de l'événement Firehose. Remplacez *EventDestination* par le nom de la destination de l'événement Firehose.

2. Si nécessaire, supprimez les données que Firehose a écrites à d'autres services. Pour de plus amples informations, veuillez consulter the section called “Supprimer les données d'événement stockées”.

Supprimer les données d'événement stockées

Pour plus d'informations sur la suppression d'informations provenant d'autres AWS services, consultez les documents suivants :

- Supprimer un objet et un compartiment dans Guide de démarrage Amazon Simple Storage Service
- Supprimer un domaine OpenSearch de service dans le manuel Amazon OpenSearch Service Developer Guide
- Deleting a Cluster du Amazon Redshift Cluster Management Guide

Vous pouvez également utiliser Firehose pour diffuser des données de courrier électronique vers Splunk, un service tiers qui n'est ni pris en charge AWS ni géré dans le. AWS Management Console Pour en savoir plus sur la suppression des données dans Splunk, contactez votre administrateur système ou consultez la documentation disponible sur le site web de Splunk.

Supprimer des données relatives aux identités

Les identités incluent les adresses e-mail et les domaines que vous utilisez pour envoyer des e-mails à l'aide d'Amazon SES. Dans certaines juridictions, les adresses e-mail ou les domaines peuvent être considérés comme des données permettant d'identifier un utilisateur personnellement.

Pour supprimer une identité à l'aide de la console Amazon SES

1. Ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Sous Identity Management (Gestion des identités), effectuez l'une des actions suivantes :
   - Choisissez Domains (Domaines) si vous souhaitez supprimer un domaine.
   - Choisissez Email Addresses (Adresses e-mail) si vous souhaitez supprimer une adresse e-mail.
3. Sélectionnez l'identité que vous voulez supprimer, puis choisissez Remove (Supprimer).
4. Dans la boîte de dialogue de confirmation, choisissez Yes, Delete Identity (Oui, supprimer l'identité).

Vous pouvez également utiliser l'API Amazon SES pour supprimer des identités. La procédure suivante utilise l' AWS Command Line Interface (AWS CLI) pour interagir avec l'API Amazon SES. Vous pouvez également interagir avec l'API à l'aide d'un AWS SDK ou en effectuant directement des requêtes HTTP.

Pour supprimer une identité à l'aide du AWS CLI

- Sur la ligne de commande, entrez la commande suivante :

  ```
  aws ses delete-identity --identity sender@example.com
  ```

  Dans cette commande, remplacez *sender@example.com* par l'identité que vous souhaitez supprimer.

Supprimer des données d'authentification d'expéditeur

L'authentification d'expéditeur fait référence au fait de configurer Amazon SES pour qu'un autre utilisateur puisse envoyer des e-mails en votre nom. Pour activer l'autorisation de l'expéditeur, vous devez créer une stratégie, comme décrit dans Utilisation de l'autorisation d'envoi avec Amazon SES.

Ces politiques contiennent des identités (qui vous appartiennent), en plus AWS des identifiants (qui sont associés à la personne ou au groupe qui envoie des e-mails en votre nom). Vous pouvez supprimer ces données personnelles en modifiant ou supprimant les stratégies d'authentification de l'expéditeur. Les procédures suivantes vous montrent comment supprimer ces stratégies.

Pour supprimer une stratégie d'authentification d'expéditeur à l'aide de la console Amazon SES

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/ses/.
2. Sous Identity Management (Gestion des identités), effectuez l'une des actions suivantes :
   - Choisissez Domains (Domaines) si la stratégie d'authentification d'expéditeur que vous souhaitez supprimer est associée à un domaine.
   - Choisissez Email Addresses (Adresses e-mail) si la stratégie d'authentification d'expéditeur que vous souhaitez supprimer est associée à une adresse e-mail.
3. Sous Identity Policies (Stratégies d'identité), sélectionnez la stratégie que vous souhaitez supprimer, puis choisissez Remove Policy (Supprimer la stratégie).

Vous pouvez également utiliser l'API Amazon SES pour supprimer des stratégies d'authentification d'expéditeur. La procédure suivante utilise le AWS Command Line Interface (AWS CLI) pour interagir avec l'API Amazon SES. Vous pouvez également interagir avec l'API à l'aide d'un AWS SDK ou en effectuant directement des requêtes HTTP.

Pour supprimer une politique d'authentification de l'expéditeur à l'aide du AWS CLI

- Sur la ligne de commande, entrez la commande suivante :

  ```
  aws ses delete-identity-policy --identity example.com --policy-name samplePolicy
  ```

  Dans cette commande, remplacez *example.com* par l'identité contenant la stratégie d'authentification d'expéditeur. Remplacez *samplePolicy* par le nom de la stratégie d'authentification d'expéditeur.

Supprimer des données relatives aux règles de réception

Si vous utilisez Amazon SES pour recevoir des e-mails entrants, vous pouvez créer des règles de réception qui sont appliquées à une ou plusieurs identités (domaines ou adresses e-mail). Ces règles déterminent comment Amazon SES traite les e-mails entrants envoyés aux identités spécifiées.

Pour supprimer une règle de réception à l'aide de la console Amazon SES

1. Ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Sous Email Receiving (Réception d'e-mails), choisissez Rule Sets (Ensembles de règles).
3. Si la règle de réception fait partie de l'ensemble de règles actif, choisissez View Active Rule Set (Afficher l'ensemble de règles actif). Sinon, sélectionnez l'ensemble de règles qui contient la règle de réception à supprimer.
4. Dans la liste des règles de réception, sélectionnez celle que vous souhaitez supprimer.
5. Dans le menu Actions, sélectionnez Delete (Supprimer).
6. Dans la boîte de dialogue de confirmation, choisissez Delete (Supprimer).

Vous pouvez également utiliser l'API Amazon SES pour supprimer des règles de réception. La procédure suivante utilise le AWS Command Line Interface (AWS CLI) pour interagir avec l'API Amazon SES. Vous pouvez également interagir avec l'API à l'aide d'un AWS SDK ou en effectuant directement des requêtes HTTP.

Pour supprimer une règle de réception à l'aide du AWS CLI

- Sur la ligne de commande, entrez la commande suivante :

  ```
  aws ses delete-receipt-rule --rule-set myRuleSet --rule-name myReceiptRule
  ```

  Dans cette commande, remplacez *myRuleSet*par le nom du jeu de règles de réception qui contient la règle de réception. *myReceiptRule*Remplacez-le par le nom de la règle de réception que vous souhaitez supprimer.

Supprimer des données relatives à des filtres d'adresses IP

Si vous utilisez Amazon SES pour recevoir des e-mails entrants, vous pouvez créer des filtres pour explicitement accepter ou bloquer les messages qui sont envoyés à partir d'adresses IP spécifiques.

Pour supprimer un filtre d'adresses IP à l'aide de la console Amazon SES

1. Ouvrez la console Amazon SES à l'adresse https://console.aws.amazon.com/ses/.
2. Sous Email Receiving (Réception d'e-mails), choisissez IP Address Filters (Filtres d'adresses IP).

3. Dans la liste des filtres d'adresses IP, sélectionnez le filtre que vous souhaitez supprimer, puis choisissez Delete (Supprimer).

Vous pouvez également utiliser l'API Amazon SES pour supprimer des filtres d'adresses IP. La procédure suivante utilise le AWS Command Line Interface (AWS CLI) pour interagir avec l'API Amazon SES. Vous pouvez également interagir avec l'API à l'aide d'un AWS SDK ou en effectuant directement des requêtes HTTP.

Pour supprimer un filtre d'adresse IP à l'aide du AWS CLI

- Sur la ligne de commande, entrez la commande suivante :

  ```
  aws ses delete-receipt-filter --filter-name IPfilter
  ```

  Dans cette commande, remplacez *IPfilter* par le nom du filtre d'adresses IP que vous souhaitez supprimer.

Supprimer des données dans les modèles d'e-mail

Si vous utilisez des modèles d'e-mail pour envoyer des messages, il est possible que ces modèles contiennent des données personnelles, en fonction de la manière dont vous les avez configurés. Par exemple, vous avez peut-être ajouté dans le modèle une adresse e-mail que les destinataires peuvent contacter pour obtenir plus d'informations.

La suppression des modèles d'e-mail est possible uniquement via l'API Amazon SES.

Pour supprimer un modèle d'e-mail à l'aide du AWS CLI

- Sur la ligne de commande, entrez la commande suivante :

  ```
  aws ses delete-template --template-name sampleTemplate
  ```

  Dans cette commande, remplacez *sampleTemplate* par le nom du modèle d'e-mail que vous souhaitez supprimer.

Supprimer des données dans des modèles d'e-mail de vérification personnalisé

Si vous utilisez des modèles personnalisés pour vérifier les nouvelles adresses d'envoi d'e-mails, il est possible que ces modèles contiennent des données personnelles, en fonction de la manière dont vous les avez configurés. Par exemple, vous avez peut-être ajouté dans le modèle d'e-mail de vérification une adresse e-mail que les destinataires peuvent contacter pour obtenir plus d'informations.

La suppression des modèles d'e-mail de vérification personnalisé est possible uniquement via l'API Amazon SES.

Pour supprimer un modèle d'e-mail de vérification personnalisé à l'aide du AWS CLI

- Sur la ligne de commande, entrez la commande suivante :

  ```
  aws ses delete-custom-verification-email-template --template-
  name verificationEmailTemplate
  ```

  Dans cette commande, remplacez *verificationEmailTemplate*par le nom du modèle d'e-mail de vérification personnalisé que vous souhaitez supprimer.

Supprimer toutes les données personnelles en fermant votre AWS compte

Il est également possible de supprimer toutes les données personnelles stockées dans Amazon SES en fermant votre compte AWS . Toutefois, cette action supprime également toutes les autres données, personnelles ou non, que vous avez stockées dans tous les autres services. AWS

Lorsque vous fermez votre AWS compte, les données de AWS celui-ci sont conservées pendant 90 jours. À l'issue de cette période de conservation, elles sont supprimées définitivement et de manière irréversible.

Pour fermer votre AWS compte

Vous trouverez des instructions complètes sur la façon de fermer votre AWS compte dans la section Fermer un AWS compte.

Gestion des identités et des accès dans Amazon SES

Vous pouvez utiliser AWS Identity and Access Management (IAM) avec Amazon Simple Email Service (Amazon SES) pour spécifier les actions d'API SES qu'un utilisateur, un groupe ou un

rôle peut effectuer. (Dans cette rubrique, nous nous référons à ces entités collectivement comme utilisateur.) Vous pouvez également contrôler les adresses électroniques que l'utilisateur peut utiliser pour le destinataire « From » et les adresses « Return-Path (Chemin de retour) » des e-mails.

Par exemple, vous pouvez créer une stratégie IAM permettant aux utilisateurs de votre organisation d'envoyer des e-mails, mais pas d'exécuter des actions administratives comme la vérification des statistiques d'envoi. Autre exemple, vous pouvez écrire une stratégie qui permet à un utilisateur d'envoyer des emails via SES à partir de votre compte, mais uniquement s'ils utilisent une adresse d'expédition spécifique.

Pour utiliser IAM, vous définissez une stratégie IAM, qui est un document définissant explicitement les autorisations et attachez la stratégie à un utilisateur. Pour savoir comment créer des stratégies IAM, consultez le guide de l'utilisateur IAM. En dehors de l'application des restrictions que vous définissez dans votre stratégie, il n'y a pas de modifications sur la façon dont les utilisateurs interagissent avec SES ou dans la façon dont SES exécute les demandes.

> **Note**
>
> - Si votre compte se trouve dans l'application de données (sandbox) SES, ses restrictions empêchent la mise en œuvre de certaines de ces politiques. Voir Demander un accès de production.
> - Vous pouvez également contrôler l'accès à SES en utilisant les stratégies d'autorisation d'envoi. Si les stratégies IAM limitent les actions que les utilisateurs peuvent effectuer, les stratégies d'autorisation d'envoi limitent la façon dont les identités vérifiées peuvent être utilisées. De plus, seules les stratégies d'autorisation d'envoi peuvent accorder l'accès entre comptes. Pour en savoir plus sur l'autorisation d'envoi, consultez Utilisation de l'autorisation d'envoi avec Amazon SES.

Si vous recherchez des informations sur la manière de générer des informations d'identification SMTP SES pour un utilisateur, consultez Obtention des informations d'identification SMTP Amazon SES.

Création de stratégies IAM pour l'accès à SES

Cette section explique comment vous pouvez utiliser les stratégies IAM plus particulièrement avec SES. Pour apprendre à créer des stratégies IAM en général, consultez le guide de l'utilisateur IAM.

Il existe trois raisons pour utiliser IAM avec SES :

- Limiter l'action d'envoi d'e-mails.
- Limiter les adresses « From », destinataire et « Return-Path (Chemin de retour) » des e-mails que l'utilisateur envoie.
- Contrôler les aspects généraux de l'utilisation de l'API tels que la durée pendant laquelle un utilisateur est autorisé à appeler l'API qu'il est habilité à utiliser.

Restriction de l'action

Pour contrôler quelles actions SES un utilisateur peut effectuer, vous utilisez l'élément `Action` d'une stratégie IAM. Vous pouvez définir l'élément `Action` sur n'importe quelle action d'API SES en préfixant le nom d'API avec la chaîne en minuscules `ses:`. Par exemple, vous pouvez définir `Action` sur `ses:SendEmail`, `ses:GetSendStatistics` ou `ses:*` (pour toutes les actions).

Ensuite, selon `Action`, spécifiez l'élément `Resource` comme suit :

Si l'élément **`Action`** n'autorise l'accès qu'aux API d'envoi d'e-mails (c'est-à-dire, **`ses:SendEmail`** et/ou **`ses:SendRawEmail`**) :

- Pour autoriser l'utilisateur à envoyer à partir de n'importe quelle identité figurant dans le vôtre Compte AWS, réglez `Resource` sur *
- Pour restreindre les identités à partir desquelles un utilisateur est autorisé à effectuer des envois, définissez `Resource` sur les ARN des identités que vous autorisez l'utilisateur à employer.

Si l'élément **`Action`** autorise l'accès à toutes les API :

- Si vous ne souhaitez pas restreindre les identités à partir desquelles l'utilisateur peut effectuer des envois, définissez `Resource` sur *
- Si vous souhaitez restreindre les identités à partir desquelles un utilisateur est autorisé à effectuer des envois, vous devez créer deux stratégies (ou deux instructions dans une stratégie) :
  - Un avec `Action` défini sur une liste explicite des non-email-sending API autorisées et `Resource` défini sur *
  - L'une avec `Action` définie sur l'une des API d'envoi d'e-mails (`ses:SendEmail` et/ou `ses:SendRawEmail`) et `Resource` défini sur l'ARN ou les ARN des identités que vous autorisez l'utilisateur à utiliser.

Pour obtenir la liste des actions SES disponibles, consultez le document Référence d'API Amazon Simple Email Service. Si l'utilisateur se sert de l'interface SMTP, vous devez autoriser l'accès à `ses:SendRawEmail` au minimum.

Restriction des adresses e-mail

Si vous voulez restreindre l'utilisateur à certaines adresses e-mail, vous pouvez utiliser un bloc `Condition`. Dans le bloc `Condition`, vous spécifiez les conditions à l'aide de clés de condition comme décrit dans le guide de l'utilisateur IAM. En utilisant les clés de condition, vous pouvez contrôler les adresses électroniques suivantes :

> **Note**
>
> Ces clés de condition d'adresse e-mail s'appliquent uniquement aux API indiquées dans le tableau suivant.

Clé de condition	Description	API
`ses:Recipients`	Restreint les adresses des destinataires, qui incluent les adresses « To: », « CC » et « BCC ».	`SendEmail` , `SendRawEmail`
`ses:FromAddress`	Limite l'adresse d'expédition.	`SendEmail` , `SendRawEmail` , `SendBounce`
`ses:FromDisplayName`	Limite l'adresse d'expédition utilisée comme nom d'affichage.	`SendEmail` , `SendRawEmail`
`ses:FeedbackAddress`	Limite l'adresse « Return-Path (Chemin de retour) », qui est l'adresse à laquelle les retours à l'expéditeur et les réclamations peuvent vous être envoyés via le transfert de commentaires par e-mail.	`SendEmail` , `SendRawEmail`

Clé de condition	Description	API
	Pour en savoir plus sur le transfert de commentaires par e-mail, consultez Réception des notifications Amazon SES par e-mail.	

Restriction par la version de l'API SES

En utilisant la clé `ses:ApiVersion` dans les conditions, vous pouvez restreindre l'accès à SES en fonction de la version de l'API SES.

> **Note**
>
> L'interface SMTP SES utilise l'API SES version 2 de `ses:SendRawEmail`.

Restriction de l'utilisation de l'API générale

En utilisant des AWS touches « wide » dans certaines conditions, vous pouvez restreindre l'accès à SES en fonction d'aspects tels que la date et l'heure auxquelles l'utilisateur est autorisé à accéder aux API. SES implémente uniquement les clés AWS de politique générales suivantes :

- `aws:CurrentTime`
- `aws:EpochTime`
- `aws:SecureTransport`
- `aws:SourceIp`
- `aws:SourceVpc`
- `aws:SourceVpce`
- `aws:UserAgent`
- `aws:VpcSourceIp`

Pour en savoir plus sur ces clés, consultez le guide de l'utilisateur IAM.

Exemples de stratégies IAM pour SES

Cette rubrique fournit des exemples de stratégies qui permettent un accès utilisateur à SES, mais uniquement sous certaines conditions.

Exemples de stratégie dans cette section :

- Autorisation de l'accès complet à toutes les actions SES
- Autorisation de l'accès à l'API SES version 2 uniquement
- Autorisation de l'accès aux actions d'envoi d'e-mail uniquement
- Restriction de la période d'envoi
- Restriction des adresses des destinataires
- Restriction de l'adresse d'expédition
- Restriction du nom d'affichage de l'expéditeur de l'e-mail
- Restriction de la destination des commentaires de retour à l'expéditeur et de réclamation

Autorisation de l'accès complet à toutes les actions SES

La stratégie suivante permet à un utilisateur d'appeler n'importe quelle action SES.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:*"
      ],
      "Resource":"*"
    }
  ]
}
```

Autorisation de l'accès à l'API SES version 2 uniquement

La stratégie suivante permet à un utilisateur d'appeler uniquement les actions SES de l'API version 2.

```
{
                    "Version":"2012-10-17",
```

```
                    "Statement":[
                        {
                            "Effect":"Allow",
                            "Action":[
                            "ses:*"
                            ],
                            "Resource":"*",
                            "Condition": {
                                "StringEquals" : {
                                "ses:ApiVersion" : "2"
                                }
                            }
                        }
                    ]
                }
```

Autorisation de l'accès aux actions d'envoi d'e-mail uniquement

La stratégie suivante permet à un utilisateur d'envoyer des e-mails avec SES, mais ne permet pas à l'utilisateur d'exécuter des actions administratives, telles que l'accès aux statistiques d'envoi SES.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource":"*"
    }
  ]
}
```

Restriction de la période d'envoi

La stratégie suivante permet à un utilisateur d'appeler les API d'envoi d'e-mails SES uniquement pendant le mois de septembre 2018.

```
{
  "Version":"2012-10-17",
```

```
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource":"*",
      "Condition":{
        "DateGreaterThan":{
          "aws:CurrentTime":"2018-08-31T12:00Z"
        },
        "DateLessThan":{
          "aws:CurrentTime":"2018-10-01T12:00Z"
        }
      }
    }
  ]
}
```

Restriction des adresses des destinataires

La stratégie suivante permet à un utilisateur d'appeler les API SES d'envoi d'e-mails, mais uniquement pour les adresses de destinataires du domaine example.com (`StringLike` est sensible à la casse).

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource":"*",
      "Condition":{
        "ForAllValues:StringLike":{
          "ses:Recipients":[
            "*@example.com"
          ]
        }
      }
```

```
    }
  ]
}
```

Restriction de l'adresse d'expédition

La stratégie suivante permet à un utilisateur d'appeler les API SES d'envoi d'e-mails, mais uniquement si l'adresse d'expédition est marketing@example.com.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource":"*",
      "Condition":{
        "StringEquals":{
          "ses:FromAddress":"marketing@example.com"
        }
      }
    }
  ]
}
```

La politique suivante permet à un utilisateur d'appeler l'SendBounceAPI, mais uniquement si l'adresse « De » est bounce@example.com.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendBounce"
      ],
      "Resource":"*",
      "Condition":{
        "StringEquals":{
```

```
          "ses:FromAddress":"bounce@example.com"
        }
      }
    }
  ]
}
```

Restriction du nom d'affichage de l'expéditeur de l'e-mail

La stratégie suivante permet à un utilisateur d'appeler les API Amazon SES d'envoi d'e-mails, mais uniquement si le nom d'affichage de l'adresse d'expédition inclut Marketing (`StringLike` est sensible à la casse).

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource":"*",
      "Condition":{
        "StringLike":{
          "ses:FromDisplayName":"Marketing"
        }
      }
    }
  ]
}
```

Restriction de la destination des commentaires de retour à l'expéditeur et de réclamation

La stratégie suivante permet à un utilisateur d'appeler les API SES d'envoi d'e-mails, mais uniquement si l'adresse « Return-Path (Chemin de retour) » de l'e-mail est feedback@example.com.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
```

```
      "Effect":"Allow",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource":"*",
      "Condition":{
        "StringEquals":{
          "ses:FeedbackAddress":"feedback@example.com"
        }
      }
    }
  ]
}
```

AWS politiques gérées pour Amazon Simple Email Service

Pour ajouter des autorisations aux utilisateurs, aux groupes et aux rôles, il est plus facile d'utiliser des politiques AWS gérées que de les rédiger vous-même. Il faut du temps et de l'expertise pour créer des politiques gérées par le client IAM qui ne fournissent à votre équipe que les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques AWS gérées. Ces politiques couvrent les cas d'utilisation courants et sont disponibles dans votre AWS compte. Pour plus d'informations sur les politiques AWS gérées, voir les politiques AWS gérées dans le guide de l'utilisateur IAM.

AWS les services maintiennent et mettent à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services ajoutent parfois des autorisations supplémentaires à une politique AWS gérée pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont plus susceptibles de mettre à jour une politique AWS gérée lorsqu'une nouvelle fonctionnalité est lancée ou lorsque de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques n'endommageront donc pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique ReadOnlyAccess AWS gérée fournit un accès en lecture seule à tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité, il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page politiques gérées par AWS pour les fonctions de tâche dans le Guide de l'utilisateur IAM.

AWS politique gérée : AmazonSES FullAccess

Vous pouvez associer la politique `AmazonSESFullAccess` à vos identités IAM. Fournit un accès complet à Amazon SES.

Pour consulter les autorisations associées à cette politique, consultez AmazonSES FullAccess dans le manuel AWS Managed Policy Reference.

AWS politique gérée : AmazonSES ReadOnlyAccess

Vous pouvez associer la politique `AmazonSESReadOnlyAccess` à vos identités IAM. Fournit un accès en lecture seule à Amazon SES.

Pour consulter les autorisations associées à cette politique, consultez AmazonSES ReadOnlyAccess dans le manuel AWS Managed Policy Reference.

AWS politique gérée : AmazonSES ServiceRolePolicy

Vous ne pouvez pas associer `AmazonSESServiceRolePolicy` à vos entités IAM. Cette politique est associée à un rôle lié à un service qui permet à Amazon SES d'effectuer des actions en votre nom. Pour plus d'informations, consultez Autorisations de rôle liées à un service pour Amazon SES.

Pour consulter les autorisations associées à cette politique, consultez AmazonSES ServiceRolePolicy dans le manuel AWS Managed Policy Reference.

Mises à jour des politiques AWS gérées par Amazon Simple Email Service

Consultez les détails et les mises à jour des politiques AWS gérées pour Amazon Simple Email Service depuis que ce service a commencé à suivre ces modifications.

Modification	Description	Date
Amazon Simple Email Service a ajouté une nouvelle politique gérée	Amazon Simple Email Service a été ajouté `AmazonSESServiceRolePolicy` au rôle lié au service `AWSServiceRoleForAmazonSES` qui permet à SES d'effectuer des actions en votre nom	13 mai 2024

Modification	Description	Date
Amazon Simple Email Service a mis à jour une définition de politique	Amazon Simple Email Service a précisé que l'entrée précédente de ce tableau (ligne ci-dessous) était la suivante : Amazon Simple Email Service a été ajouté `ses:BatchGetMetricData` à la politique ReadOnlyAccess gérée d'Amazon. Cela donnera accès à l'API SES BatchGetMetricData	30 avril 2024
Amazon Simple Email Service a mis à jour une définition de politique	Amazon Simple Email Service a été ajouté `ses:BatchGet*` à la politique ReadOnlyAccess gérée d'Amazon : cela donnera accès à l'API SES BatchGetMetricData	16 février 2024
Amazon Simple Email Service a modifié deux définitions de politique	Amazon Simple Email Service a été supprimé « via la console AWS de gestion » à la fin des définitions d'AmazonSES FullAccess et d'ReadOnlyAccess AmazonSES	3 mai 2023
Amazon Simple Email Service a commencé à suivre les modifications	Amazon Simple Email Service a commencé à suivre les modifications apportées à ses politiques AWS gérées	5 avril 2023

Utilisation de rôles liés à un service pour Amazon SES

Amazon Simple Email Service (SES) AWS Identity and Access Management utilise des rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à Amazon SES. Les rôles liés au service sont prédéfinis par SES et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration de SES car vous n'avez pas à ajouter manuellement les autorisations nécessaires. SES définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul SES peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos ressources SES car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services prenant en charge les rôles liés à un service, consultez les AWS services opérationnels avec IAM et recherchez les services présentant la mention Yes (Oui) dans la colonne Service-linked roles (Rôles liés à un service). Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations de rôle liées à un service pour Amazon SES

SES utilise le rôle lié à un service nommé AWSServiceRoleForAmazonSES— Permet à SES de publier les mesures de surveillance CloudWatch de base d'Amazon pour le compte de vos ressources SES.

Le rôle AWSServiceRoleForAmazonSES lié à un service fait confiance au service suivant pour assumer le rôle :

- `ses.amazonaws.com`

La politique d'autorisations de rôle nommée AmazonSES ServiceRolePolicy est une politique AWS gérée qui permet à SES d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : `cloudwatch:PutMetricData` dans l'espace de `AWS/SES` CloudWatch noms. Cette action autorise SES à placer des données métriques dans l'espace de CloudWatch `AWS/SES` noms. Pour plus d'informations sur les métriques SES disponibles dans CloudWatch, voirJournalisation et surveillance dans Amazon SES.

- Action : `cloudwatch:PutMetricData` dans l'espace de `AWS/SES/MailManager` CloudWatch noms. Cette action autorise SES à placer des données métriques dans l'espace de CloudWatch `AWS/SES/MailManager` noms. Pour plus d'informations sur les métriques SES disponibles dans CloudWatch, voirJournalisation et surveillance dans Amazon SES.
- Action : `cloudwatch:PutMetricData` dans l'espace de `AWS/SES/Addons` CloudWatch noms. Cette action autorise SES à placer des données métriques dans l'espace de CloudWatch `AWS/SES/Addons` noms. Pour plus d'informations sur les métriques SES disponibles dans CloudWatch, voirJournalisation et surveillance dans Amazon SES.

Vous devez configurer les autorisations de manière à permettre à vos utilisateurs, groupes ou rôles de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour Amazon SES

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez des ressources SES dans le AWS Management Console AWS CLI, le ou l' AWS API, SES crée le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez des ressources SES, SES crée à nouveau le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour Amazon SES

SES ne vous permet pas de modifier le rôle AWSServiceRoleForAmazonSES lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM.

Supprimer un rôle lié à un service pour SES

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer votre rôle lié à un service avant de pouvoir le supprimer manuellement.

Nettoyage d'un rôle lié à un service

Avant de pouvoir utiliser IAM pour supprimer un rôle lié à un service, vous devez d'abord supprimer toutes les ressources SES.

> **Note**
>
> Si le service SES utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Suppression manuelle du rôle lié au service

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForAmazonSES service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés aux services Amazon SES

SES ne prend pas en charge l'utilisation de rôles liés à un service dans toutes les régions où le service est disponible. Vous pouvez utiliser le AWSServiceRoleForAmazonSES rôle dans les régions suivantes.

Nom de la région	Identité de la région	Support dans SES
US East (Virginie du Nord)	us-east-1	Oui
USA Est (Ohio)	us-east-2	Oui
Asie-Pacifique (Sydney)	ap-southeast-2	Oui
Asie-Pacifique (Tokyo)	ap-northeast-1	Oui
Europe (Francfort)	eu-central-1	Oui
Europe (Irlande)	eu-west-1	Oui

Journalisation et surveillance dans Amazon SES

La surveillance est une étape importante du maintien de la fiabilité, de la disponibilité et des performances d'Amazon SES et de vos solutions AWS. AWS fournit des outils pour vous aider à surveiller Amazon SES et à répondre aux éventuels incidents.

- Amazon CloudWatch contrôle vos ressources AWS et les applications que vous exécutez sur AWS en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Pour plus d'informations, consultez Récupération de données d'événements Amazon SES à partir de CloudWatch et Création d'alarmes de surveillance de réputation avec CloudWatch.
- AWS CloudTrail capture les appels d'API et les événements associés créés par votre Compte AWS ou au nom de celui-ci et livre les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été émis, ainsi que le moment où les appels ont eu lieu. Pour de plus amples informations, veuillez consulter Journalisation des appels d'API Amazon SES avec AWS CloudTrail.
- Les Événements d'envoi d'e-mails Amazon SES peuvent vous aider à affiner votre stratégie d'envoi d'e-mails. Amazon SES capture les informations détaillées, y compris les nombres d'envoi, de messages délivrés, d'ouvertures, de clics, de retours à l'expéditeur, de réclamations et de rejets. Pour de plus amples informations, veuillez consulter Surveillance de votre activité d'envoi.
- Les métriques de réputation Amazon SES suivent les taux de retour à l'expéditeur et de réclamations pour votre compte. Pour de plus amples informations, veuillez consulter Surveillance de la réputation d'expéditeur.

Journalisation des appels d'API Amazon SES avec AWS CloudTrail

Amazon S3 est intégré à AWS CloudTrail, service qui enregistre les actions effectuées par un utilisateur, un rôle ou un service AWS dans Amazon SES. CloudTrail capture les appels d'API pour Amazon SES en tant qu'événements. Ces captures incluent les appels de la console Amazon SES et les appels de code vers les opérations d'API Amazon SES. Si vous créez un journal d'activité, vous pouvez activer la livraison continue des événements CloudTrail dans un compartiment Amazon S3, y compris les événements pour Amazon SES. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Event history (Historique des événements). Avec les informations collectées par CloudTrail, vous

pouvez déterminer la demande qui a été envoyée à Amazon SES, l'adresse IP à partir de laquelle la demande a été effectuée, l'auteur et la date de la demande, ainsi que d'autres détails.

Pour en savoir plus sur CloudTrail, y compris la façon de le configurer et de l'activer, consultez le AWS CloudTrail Guide de l'utilisateur.

Informations relatives à Amazon SES dans CloudTrail

CloudTrail est activé dans votre Compte AWS lors de la création de ce dernier. Quand une activité d'événement prise en charge a lieu dans Amazon SES, elle est enregistrée dans un événement CloudTrail avec d'autres événements de service AWS dans Event history (Historique des événements). Vous pouvez afficher, rechercher et télécharger les événements récents dans votre Compte AWS. Pour de plus amples informations, veuillez consulter Affichage des événements avec l'historique des événements CloudTrail.

Pour un registre continu des événements dans votre Compte AWS, y compris les événements pour Amazon SES, créez un journal d'activité. Un journal d'activité permet à CloudTrail de distribuer les fichiers journaux vers Simple Storage Service (Amazon S3) bucket. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal de suivi consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres services AWS pour analyser et agir sur les données d'événements collectées dans les journaux CloudTrail. Pour en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité
- Intégrations et services pris en charge par CloudTrail
- Configuration des Notifications de Amazon SNS pour CloudTrail
- Réception des fichiers journaux CloudTrail de plusieurs régions et Réception des fichiers journaux CloudTrail de plusieurs comptes

Amazon SES prend en charge la journalisation de toutes les actions répertoriées dans la Référence d'API SES et la Référence d'API SES v2en tant qu'événements dans les fichiers journaux CloudTrail, sauf ceux indiqués dans la zone de notes ci-dessous :

> **Note**
>
> Amazon SES fournit des événements de gestion à CloudTrail. Les événements de gestion incluent les actions qui sont liées à la création et à la gestion des ressources dans votre

Compte AWS. Dans Amazon SES, les événements de gestion incluent des actions telles que la création et la suppression d'identités ou de règles de réception.
Les événements de gestion sont différents des événements de données. Les événements de données sont des événements qui sont liés à l'accès des données et à l'interaction avec celles-ci au sein de votre Compte AWS. Dans Amazon SES, les événements de données incluent des actions telles que l'envoi d'e-mails.
Comme Amazon SES fournit uniquement des événements de gestion à CloudTrail, les événements suivants ne sont pas enregistrés dans CloudTrail :

- SendEmail
- SendRawEmail
- SendTemplatedEmail
- SendBulkTemplatedEmail

Vous pouvez utiliser la publication d'événements pour enregistrer les événements liés à l'envoi d'e-mails. Pour de plus amples informations, veuillez consulter Surveillance de l'envoi d'e-mails à l'aide de la publication d'événements Amazon SES.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre service AWS.

Pour en savoir plus, consultez l'élément userIdentity CloudTrail.

Exemple : entrées du fichier journal Amazon SES

Un journal d'activité est une configuration qui permet d'envoyer des événements sous forme de fichiers journaux à un compartiment Simple Storage Service (Amazon S3) que vous spécifiez. Les fichiers journaux CloudTrail peuvent contenir une ou plusieurs entrées. Un événement représente une demande unique provenant de n'importe quelle source et comprend des informations sur l'action

demandée, la date et l'heure de l'action, les paramètres de la requête, etc. Les fichiers journaux CloudTrail ne constituent pas une série ordonnée retraçant les appels d'API publiques. Ils ne suivent aucun ordre précis.

L'exemple suivant montre une entrée de journal CloudTrail qui illustre les actions `DeleteIdentity` et `VerifyEmailIdentity`.


```
{
  "Records":[
    {
      "awsRegion":"us-west-2",
      "eventID":"0ffa308d-1467-4259-8be3-c749753be325",
      "eventName":"DeleteIdentity",
      "eventSource":"ses.amazonaws.com",
      "eventTime":"2018-02-02T21:34:50Z",
      "eventType":"AwsApiCall",
      "eventVersion":"1.02",
      "recipientAccountId":"111122223333",
      "requestID":"50b87bfe-ab23-11e4-9106-5b36376f9d12",
      "requestParameters":{
        "identity":"amazon.com"
      },
      "responseElements":null,
      "sourceIPAddress":"192.0.2.0",
      "userAgent":"aws-sdk-java/unknown-version",
      "userIdentity":{
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "accountId":"111122223333",
        "arn":"arn:aws:iam::111122223333:root",
        "principalId":"111122223333",
        "type":"Root"
      }
    },
    {
      "awsRegion":"us-west-2",
      "eventID":"5613b0ff-d6c6-4526-9b53-a603a9231725",
      "eventName":"VerifyEmailIdentity",
      "eventSource":"ses.amazonaws.com",
      "eventTime":"2018-02-04T01:05:33Z",
      "eventType":"AwsApiCall",
      "eventVersion":"1.02",
      "recipientAccountId":"111122223333",
      "requestID":"eb2ff803-ac09-11e4-8ff5-a56a3119e253",
```

```
      "requestParameters":{
        "emailAddress":"sender@example.com"
      },
      "responseElements":null,
      "sourceIPAddress":"192.0.2.0",
      "userAgent":"aws-sdk-java/unknown-version",
      "userIdentity":{
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "accountId":"111122223333",
        "arn":"arn:aws:iam::111122223333:root",
        "principalId":"111122223333",
        "type":"Root"
      }
    }
  ]
}
```


Validation de la conformité pour Amazon Simple Email Service

Des auditeurs tiers évaluent la sécurité et la conformité d'mazon Simple Email Service dans le cadre de plusieurs programmes de conformité AWS. Il s'agit notamment des certifications SOC, PCI, FedRAMP, HIPAA et d'autres.

Pour obtenir une liste des services AWS relevant de programmes de conformité spécifiques, consultez Services AWS relevant de programme de conformité. Pour obtenir des renseignements généraux, consultez Programmes de conformité AWS .

Vous pouvez télécharger les rapports de l'audit externe avec AWS Artifact. Pour de plus amples informations, veuillez consulter Téléchargement de rapports dans AWS Artifact.

Votre responsabilité de conformité lors de l'utilisation d'Amazon Simple Email Service est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise, ainsi que la législation et la réglementation applicables. AWS fournit les ressources suivantes pour faciliter le respect de la conformité :

- Guides Quick Start (démarrage rapide) de la sécurité et de la conformité– Ces guides de déploiement traitent des considérations architecturales et fournissent des étapes pour déployer des environnements de base axés sur la sécurité et la conformité sur AWS.
- Livre blanc sur l'architecture pour la sécurité et la conformité HIPAA – Le livre blanc décrit comment les entreprises peuvent utiliser AWS pour créer des applications conformes à HIPAA.

- Ressources de conformité AWS – Cet ensemble de manuels et de guides peut s'appliquer à votre secteur et à votre emplacement.
- Évaluation des ressources à l'aide de règles dans le Guide du développeur AWS Config : AWS Config évalue dans quelle mesure vos configurations de ressources sont conformes aux pratiques internes, aux directives sectorielles et aux réglementations.
- AWS Security Hub : ce service AWS fournit une vue complète de votre état de sécurité au sein d'AWS qui vous permet de vérifier votre conformité aux normes du secteur et aux bonnes pratiques de sécurité.

Amazon Simple Email Service

L'infrastructure mondiale d'AWS repose sur les régions et les zones de disponibilité AWS. Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour en savoir plus sur les régions AWS et zones de disponibilité , consultez Infrastructure mondiale AWS.

Sécurité de l'infrastructure dans Amazon Simple Email Service

En tant que service géré, Amazon Simple Email Service est protégé par la sécurité du réseau mondial AWS. Pour plus d'informations sur les services de sécurité AWS et la manière dont AWS protège l'infrastructure, consultez la section Sécurité du cloud AWS. Pour concevoir votre environnement AWS en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le Security Pillar AWS Well-Architected Framework (Pilier de sécurité de l'infrastructure Well-Architected Framework).

Vous utilisez les appels d'API publiés par AWS pour accéder à Amazon Simple Email Service via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et nous recommandons TLS 1.3.

- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Configuration des points de terminaison d'un VPC avec Amazon SES

De nombreux clients Amazon SES ont mis en place des stratégies d'entreprise qui limitent la capacité de connexion de leurs systèmes internes à l'Internet public. Ces stratégies empêchent l'utilisation des points de terminaison publics Amazon SES.

Si vous avez mis en place des politiques similaires, vous pouvez travailler dans le cadre de ces restrictions en utilisant Amazon Virtual Private Cloud. Avec Amazon VPC, vous pouvez déployer AWS des ressources dans un réseau virtuel qui existe dans une zone isolée du. AWS Cloud Pour plus d'informations sur la sécurité dans Amazon VPC, veuillez consulter le Guide de l'utilisateur Amazon VPC.

Vous pouvez vous connecter directement à SES depuis Amazon VPC via un point de terminaison de VPC de manière sécurisée et scalable. Lorsque vous utilisez un point de terminaison VPC d'interface, votre posture de sécurité s'en trouve améliorée, car vous n'avez pas besoin d'ouvrir de pare-feu pour le trafic sortant, et vous bénéficiez en outre d'autres avantages liés à l'utilisation des points de terminaison Amazon VPC.

Lorsque vous utilisez un point de terminaison de VPC, le trafic vers SES ne transite pas par Internet et il ne quitte jamais le réseau Amazon, si bien que votre VPC est connecté à SES de manière sécurisée sans risques de disponibilité ni contraintes de bande passante sur votre trafic réseau. Vous pouvez centraliser SES à l'échelle de votre infrastructure multicompte et le mettre à la disposition de vos comptes sous la forme d'un service sans avoir à utiliser de passerelle Internet.

Limites

- SES ne prend pas en charge les points de terminaison d'un VPC dans les zones de disponibilité suivantes : `use1-az2`, `use1-az3`, `use1-az5`, `usw1-az2`, `usw2-az4`, `apne2-az4`, `cac1-az3` et `cac1-az4`.
- Le point de terminaison SMTP utilisé dans le VPC est limité à la Région AWS actuellement utilisée pour votre compte.

Exemple de procédure de configuration de SES dans Amazon VPC

Prérequis

Avant de commencer la procédure décrite dans cette section, vous devez effectuer les étapes suivantes :

- Si vous ne disposez pas déjà d'un cloud privé virtuel (VPC), en créer un. Vous trouverez les procédures dans la rubrique Démarrer avec Amazon VPC.
- Lancer une instance Amazon EC2 dans votre VPC pour tester la connectivité vers le point de terminaison de VPC créé dans une étape ultérieure. Pour plus d'informations, consultez VPC par défaut.

Note

Même s'il est possible d'utiliser n'importe quelle ressource avec les points de terminaison VPC pour SES, dans un souci de simplification de la méthode de test, vous utiliserez dans cet exemple une instance EC2 en guise de ressource. Comme Amazon EC2 restreint le trafic d'e-mails sur le port 25 par défaut, vous devrez utiliser un autre port que le TCP 25, par exemple le TCP 465, 587, 2465 ou 2587.

Configuration de SES dans Amazon VPC

Le processus de configuration d'un point de terminaison de VPC en vue de son utilisation avec SES consiste en quelques étapes distinctes. En premier lieu, vous devez créer un groupe de sécurité permettant à l'instance de communiquer avec les ports SMTP, créer ensuite un point de terminaison

de VPC pour Amazon SES, et enfin tester la connexion au point de terminaison de VPC pour vérifier qu'il est correctement configuré.

Étape 1 : Créer le groupe de sécurité

Dans cette étape, vous allez créer un groupe de sécurité qui va permettre aux instances Amazon EC2 de communiquer avec les points de terminaison de l'interface VPC que vous allez créer.

Pour créer le groupe de sécurité

1. Dans le panneau de navigation de la console Amazon EC2, sous Réseau et sécurité, choisissez Groupes de sécurité.
2. Sélectionnez Create security group (Créer un groupe de sécurité).
3. Sous Basic details (Détails de base), procédez comme suit :
   - Pour Nom du groupe de sécurité (Security group name), entrez un nom unique qui identifie le groupe de sécurité.
   - Pour Description, entrez un texte décrivant l'objectif du groupe de sécurité.
   - Pour VPC, choisissez le VPC dans lequel vous souhaitez utiliser Amazon SES.
4. Pour Inbound rules (Règles entrantes), choisissez Add rule (Ajouter une règle).
5. Pour la nouvelle Règle entrante, procédez comme suit :
   - Pour Type, choisissez Custom TCP (TCP personnalisé).
   - Pour Port range (Plage de ports), entrez le numéro de port que vous souhaitez utiliser pour envoyer des e-mails. Vous pouvez utiliser l'un des numéros de port suivants : **465**, **587**, **2465** ou **2587**.
   - Pour Source type (Type de source), choisissez Personnalisé.
   - Dans le champ Source, saisissez la plage CIDR d'adresses IP privées ou d'autres ID de groupe de sécurité qui contiennent les ressources dont se servira le point de terminaison de VPC pour communiquer avec le service SES.
   - (Répétez les étapes 4 à 5 pour chaque plage CIDR ou groupe de sécurité depuis lesquels l'accès doit être autorisé.)
6. Lorsque vous avez terminé, choisissez Create security group (Créer un groupe de sécurité).

Étape 2 : Créer le point de terminaison de VPC

Dans Amazon VPC, un point de terminaison VPC vous permet de connecter votre VPC aux services pris en charge. AWS Dans cet exemple, vous allez configurer Amazon VPC de façon à permettre à votre groupe de sécurité Amazon EC2 de se connecter à Amazon SES.

Pour créer le point de terminaison d'un VPC

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Sous Virtual Private Cloud (Cloud privé virtuel), choisissez Endpoints (Points de terminaison).
3. Choisissez Create Endpoint (Créer un point de terminaison) pour ouvrir la page Create Endpoint (Créer un point de terminaison).
4. (Facultatif) Dans le volet Endpoint settings (Paramètres du point de terminaison), créez une balise dans le champ Name tag (Nommer la balise).
5. Pour Catégorie de service, sélectionnez Services AWS .
6. Dans le volet Services, filtrez smtp dans la barre de recherche, puis sélectionnez la case d'option correspondante.
7. Dans le volet VPC, cliquez dans la barre de recherche et sélectionnez un VPC dans la zone de liste (consultez the section called “Prérequis”).
8. Dans le volet Subnets (Sous-réseaux), sélectionnez Availability Zones (Zones de disponibilité) et Subnet IDs (ID de sous-réseau).

   > **Note**
   >
   > Amazon SES ne prend pas en charge les points de terminaison d'un VPC dans les zones de disponibilité suivantes : `use1-az2`, `use1-az3`, `use1-az5`, `usw1-az2`, `usw2-az4`, `apne2-az4`, `cac1-az3` et `cac1-az4`.

9. Dans le volet Security groups (Groupes de sécurité), sélectionnez le groupe de sécurité créé plus tôt.
10. (Facultatif) Dans le volet Balises, vous pouvez créer une ou plusieurs balises.
11. Choisissez Créer un point de terminaison. Attendez environ cinq minutes pendant qu'Amazon VPC crée le point de terminaison. Lorsque le point de terminaison est prêt à être utilisé, la valeur de la colonne Status (Statut) devient Available (Disponible).

(Facultatif) Étape 3 : Tester la connexion au point de terminaison de VPC

Une fois parvenu à la fin du processus de configuration du point de terminaison de VPC, vous pouvez tester la connexion pour vérifier que le point de terminaison de VPC est correctement configuré. Vous pouvez tester la connexion à l'aide des outils de ligne de commande fournis avec la plupart des systèmes d'exploitation.

Pour tester la connexion au point de terminaison de VPC

1. Lancez une instance Amazon EC2 dans le VPC où vous venez de créer le point de terminaison de VPC email-smtp.

   Pour plus d'informations sur la connexion aux instances Linux, consultez la section Se connecter à votre instance Linux dans le guide de l'utilisateur Amazon EC2.

   Pour plus d'informations sur la connexion aux instances Windows, consultez le didacticiel de mise en route du guide de l'utilisateur Amazon EC2.
2. Envoyez un e-mail de test, par exemple à l'aide de l'interface SMTP SES.

> **Note**
>
> Vous devez vérifier une adresse e-mail ou un domaine pour pouvoir envoyer des e-mails via Amazon SES. Pour plus d'informations sur la vérification des identités, veuillez consulter Vérification des identités dans Amazon SES.

Dépannage des problèmes Amazon SES

Cette section contient les rubriques suivantes, qui peuvent vous être utiles lorsque vous rencontrez des problèmes :

- Pour obtenir des informations sur les problèmes de vérification de domaine que vous êtes susceptible de rencontrer, consultez Problèmes de vérification d'adresse e-mail et de domaine.
- Pour obtenir des solutions aux problèmes liés à la fonction DKIM, veuillez consulter Résolution des problèmes liés à la fonction DKIM dans Amazon SES.
- Pour obtenir une liste des problèmes de remise courants que vous êtes susceptible de rencontrer lorsque vous envoyez des e-mails, ainsi que les mesures correctives que vous pouvez prendre, consultez Problèmes de remise Amazon SES.
- Pour obtenir une description des problèmes que les destinataires peuvent rencontrer lors de la réception d'un e-mail envoyé via Amazon SES, consultez Problèmes au niveau des e-mails reçus d'Amazon SES.
- Pour trouver des solutions aux problèmes liés aux notifications de retour à l'expéditeur, de réclamation et de message délivré, consultez Problèmes de notifications Amazon SES.
- Pour obtenir une liste d'erreurs qui peuvent se produire lorsque vous envoyez un e-mail avec Amazon SES, consultez Erreurs d'envoi d'e-mails Amazon SES.
- Pour obtenir des conseils sur la manière d'accélérer l'envoi de vos e-mails lorsque vous effectuez plusieurs appels à Amazon SES à l'aide de l'API ou de l'interface SMTP, consultez Accroissement du débit avec Amazon SES.
- Pour obtenir des solutions aux problèmes courants que vous pouvez rencontrer lorsque vous utilisez Amazon SES via son interface SMTP (Simple Mail Transfer Protocol), ainsi qu'une liste des codes de réponse SMTP Amazon SES renvoyés, veuillez consulter Problèmes SMTP Amazon SES.
- Pour obtenir une liste des codes d'erreur courants renvoyés par l'API Amazon SES v2, consultez Erreurs courantes.
- Pour obtenir une description des problèmes courants liés à nos processus d'envoi, et savoir comment les traiter, veuillez consulter FAQ sur le processus de vérification des envois Amazon SES.
- Pour savoir comment les listes DNSBL (DNS-based Blackhole Lists) affectent vos envois avec Amazon SES, consultez FAQ sur les listes DNSBL (DNS Blackhole Lists).

Si vous appelez l'API Amazon SES, consultez le document Référence d'API Amazon Simple Email Service pour découvrir les erreurs HTTP que vous êtes susceptible de recevoir.

> **Note**
>
> Si vous avez besoin d'une assistance technique, n'utilisez pas le lien d'envoi de commentaires présent sur les pages de ce guide du développeur, car le formulaire est envoyé à l'équipe de documentation AWS, et non à AWS Support. Explorez plutôt les différentes options d'assistance disponibles sur la page Contactez-nous.

Table des matières

Problèmes généraux relatifs à Amazon SES

Les informations contenues dans cette page expliquent et aident à diagnostiquer les problèmes que vous pouvez rencontrer lors de l'utilisation d'Amazon SES.

Les modifications que j'apporte ne sont pas visibles immédiatement

En tant que service auquel on accède avec des ordinateurs situés dans des centres de données du monde entier, Amazon SES utilise un modèle d'informatique distribuée appelé cohérence éventuelle. Les modifications que vous apportez à Amazon SES (ou à d'autres services AWS) nécessitent un certain temps avant de devenir visibles depuis tous les points de terminaison possibles. Une partie du retard s'explique par le temps requis pour envoyer les données d'un serveur à un autre, d'une région du monde à une autre. Dans la plupart des cas, ce retard se limitera à quelques minutes.

Il peut être observé notamment dans les cas suivants :

- Création et modification de jeux de configurations – Lorsque vous créez ou modifiez un jeu de configurations (par exemple, si vous associez un groupe d'adresses IP dédiées à un jeu de configurations existant), un bref laps de temps peut être observé entre le moment où vous le créez ou le modifiez et le moment où ces modifications sont actives.
- Création et modification de destinations d'événement – Lorsque vous créez ou modifiez une destination d'événement (par exemple, pour donner instruction à Amazon SES d'envoyer vos données d'envoi d'e-mails à un autre service AWS), un certain laps de temps peut s'écouler entre le moment où vous créez ou modifiez la destination d'événement et le moment où l'événement d'envoi d'e-mail parvient effectivement à la destination spécifiée.

Problèmes de vérification d'adresse e-mail et de domaine

Pour vérifier une adresse e-mail ou un domaine avec Amazon SES, vous devez lancer le processus à partir de la console Amazon SE; ou de l'API Amazon SES. Cette section contient des informations qui peuvent vous aider à résoudre les problèmes liés au processus de vérification.

> **Note**
>
> Dans les procédures suivantes, la référence aux enregistrements DNS peut faire référence à des enregistrements CNAME ou TXT en fonction de la forme de DKIM utilisée. Easy DKIM utilise des enregistrements CNAME et Bring Your Own DKIM (BYODKIM) utilise des enregistrements TXT. Des procédures de vérification détaillées sont fournies pour chacun desEasy DKIMouPAR ODKIM.

Problèmes courants de vérification de domaine

Si vous essayez de vérifier un domaine à l'aide de la procédure décrite dans the section called “Vérification d'une identité de domaine” et que vous rencontrez des problèmes, passez en revue les causes et les solutions possibles ci-dessous.

- Vous essayez de vérifier un domaine qui ne vous appartient pas – Vous ne pouvez pas vérifier un domaine qui ne vous appartient pas. Par exemple, si vous souhaitez envoyer des e-mails via Amazon SES à partir d'une adresse sur le domaine gmail.com, vous devez vérifier cette adresse e-mail proprement dite. Vous ne pouvez pas vérifier la totalité du domaine gmail.com.

- Vous essayez de vérifier un domaine privé – Vous ne pouvez pas vérifier un domaine si les enregistrements DNS ne peuvent pas être résolus via un DNS public.
- Votre fournisseur DNS n'accepte pas les traits de soulignement dans les noms de registres DNS – Un petit nombre de fournisseurs DNS ne vous permettent pas d'inclure le caractère de soulignement dans les noms de registre pour votre domaine. Cependant, les traits de soulignement dans les noms de registres DKIM sont obligatoires. Si votre fournisseur DNS ne vous permet pas de saisir un caractère de soulignement dans le nom de registre, contactez l'équipe de support client du fournisseur pour obtenir de l'aide.
- Votre fournisseur DNS a ajouté le nom de domaine à la fin de le registre DNS – Certains fournisseurs DNS ajoutent automatiquement le nom de votre domaine au nom d'attribut de le registre DNS. Par exemple, si vous créez un registre où le nom d'attribut est _domainkey.exemple.com, le fournisseur peut ajouter le nom de domaine, ce qui donne _domainkey.exemple.com.exemple.com. Pour éviter la duplication du nom de domaine, ajoutez un point à la fin du nom de domaine dans l'enregistrement DNS. Cette étape indique à votre fournisseur DNS qu'il n'est pas nécessaire d'ajouter le nom de domaine à le registre TXT.
- Votre fournisseur DNS a modifié la valeur de registre DNS – Certains fournisseurs modifient automatiquement les valeurs de registre DNS pour n'utiliser que des lettres minuscules. Amazon SES vérifie uniquement votre domaine lorsqu'il détecte un registre de vérification dont la valeur d'attribut correspond exactement à celle qu'Amazon SES a fournie lorsque vous avez lancé le processus de vérification de domaine. Si le fournisseur DNS pour votre domaine modifie les valeurs de votre enregistrement TXT pour utiliser uniquement des lettres minuscules, contactez le fournisseur DNS pour obtenir plus d'aide.
- Vous souhaitez vérifier un même domaine plusieurs fois – Vous pouvez être amené à vérifier votre domaine plusieurs fois, car vous effectuez des envois dans différentes régions ou parce que vous utilisez le même domaine pour effectuer des envois à partir de plusieurs comptes AWS. Si votre fournisseur DNS ne vous autorise pas à avoir plusieurs enregistrements TXT avec le même nom d'attribut, vous pouvez quand-même vérifier deux domaines. Si votre fournisseur DNS le permet, vous pouvez affecter plusieurs valeurs d'attribut au même enregistrement TXT. Par exemple, si votre DNS est géré par Amazon Route 53, vous pouvez définir plusieurs valeurs pour le même enregistrement TXT, en respectant les étapes suivantes :

  1. Dans la console Route 53, choisissez le registre TXT que vous avez créé lorsque vous avez vérifié votre domaine dans la première région.
  2. Dans la zoneValue (Valeur), allez à la fin de la valeur d'attribut existante, puis appuyez sur Entrée.
  3. Ajoutez la valeur d'attribut de la région supplémentaire, puis enregistrez le jeu de registres.

Si votre fournisseur DNS ne vous permet pas d'affecter plusieurs valeurs d'attribut au même enregistrement TXT, vous pouvez vérifier le domaine une fois avec _amazonses dans le nom d'attribut de le registre TXT et une autre fois avec _amazonses supprimé du nom d'attribut. L'inconvénient de cette solution est que vous ne pouvez vérifier le même domaine que deux fois.

Vérification des paramètres de vérification de domaine

Vous pouvez vérifier que votre enregistrement TXT de vérification de domaine Amazon SES est correctement publié sur votre serveur DNS en utilisant la procédure suivante. Cette procédure utilise l'outil nslookup, disponible pour Windows et Linux. Sous Linux, vous pouvez également utiliser dig.

Les commandes figurant dans ces instructions ont été exécutées sur Windows 7, et l'exemple de domaine que nous utilisons est ses-example.com.

Dans cette procédure, vous trouvez d'abord les serveurs DNS qui servent votre domaine, puis interrogez ces serveurs pour afficher les enregistrements TXT. Vous interrogez les serveurs DNS qui servent votre domaine, car ces serveurs contiennent les dernières informations concernant votre domaine et qui peuvent prendre du temps à être propagées vers d'autres serveurs DNS.

Pour vérifier que votre enregistrement TXT de vérification de domaine est publié sur votre serveur DNS

1. Trouvez les serveurs de noms de votre domaine en effectuant les étapes suivantes.

   a. Accédez à la ligne de commande. Pour obtenir la ligne de commande sur Windows 7, choisissez Start (Démarrer), puis tapez cmd. Sur les systèmes d'exploitation Linux, ouvrez une fenêtre de terminal.

   b. À l'invite de commande, tapez ce qui suit, où <domain> représente votre domaine. Tous les serveurs de noms qui servent votre domaine sont alors affichés.

      ```
      nslookup -type=NS <domain>
      ```

      Si votre domaine est ses-example.com, cette commande se présente comme suit :

      ```
      nslookup -type=NS ses-example.com
      ```

Le résultat de la commande présente les serveurs de noms qui servent votre domaine. Vous interrogerez l'un de ces serveurs à l'étape suivante.

2. Vérifiez que le registre TXT est correctement publié en effectuant les étapes suivantes. N'oubliez pas qu'Amazon SES génère trois enregistrements CNAME pour l'authentification Easy DKIM. Répétez donc les procédures suivantes pour chacun des trois.

   a. À l'invite de commande, tapez ce qui suit, où <domain> représente votre domaine et <name server> représente l'un des serveurs de noms que vous avez trouvés à l'étape 1.

   ```
   nslookup -type=CNAME <random string>_domainkey.<domain> <name server>
   ```

   Dans notre exemple ses-example.com, si nous trouvions un serveur de noms appelé ns1.name-server.net à l'étape 1, nous saisirions ce qui suit :

   ```
   nslookup -type=CNAME 4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz_domainkey.ses-example.com
    ns1.name-server.net
   ```

   b. Dans le résultat de la commande, vérifiez que la chaîne qui suit `canonical name =` correspond à la valeur TXT qui s'affiche lorsque vous choisissez le domaine dans la liste des identités de la console Amazon SES.

   Dans notre exemple, nous recherchons un registre TXT sous `4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz_amazonses.ses-example.com` avec la valeur `4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz.dkim.amazonses.com`. Si le registre est correctement publié, la commande doit générer le résultat suivant :

   ```
   4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz_domainkey.ses-example.com canonical name =
    "4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz.dkim.amazonses.com"
   ```

Problèmes courants de vérification d'e-mail

- L'e-mail de vérification n'est pas arrivé – Si vous avez mené à bien les procédures décrites dans Vérification d'une identité d'adresse e-mail, mais que vous ne recevez pas l'e-mail de vérification dans les minutes qui suivent, effectuez les étapes suivantes :
  - Recherchez l'adresse e-mail que vous tentez de vérifier dans le dossier de courrier indésirable.

- Assurez-vous que l'adresse que vous essayez de vérifier est en mesure de recevoir des e-mails. Avec une adresse e-mail distincte (par exemple, votre adresse e-mail personnelle), envoyez un message à l'adresse que vous souhaitez vérifier.
- Consultez la liste des adresses vérifiées dans la console Amazon SES. Assurez-vous qu'il n'y a pas d'erreurs dans l'adresse e-mail que vous essayez de vérifier.

Résolution des problèmes liés à la fonction DKIM dans Amazon SES

Cette section répertorie certains des problèmes que vous pouvez rencontrer lorsque vous configurez l'authentification DKIM dans Amazon SES. Si vous tentez de configurer DKIM et que vous rencontrez des problèmes, examinez les causes possibles et les solutions ci-dessous.

Vous avez configuré DKIM avec succès, mais vos messages ne sont pas signés par DKIM

Si vous avez utilisé Easy DKIM ou BYODKIM pour configurer DKIM pour un domaine, mais que les messages que vous envoyez ne sont pas signés par DKIM, procédez comme suit :

- Vérifiez que la fonction DKIM est activée pour l'identité appropriée. Pour activer la fonction DKIM pour une identité dans la console Amazon SES, choisissez le domaine de messagerie dans la liste Identities (Identités). Sur la page de détails du domaine, développez DKIM, puis choisissez Enable (Activer) pour activer la fonction DKIM.
- Assurez-vous que vous n'envoyez pas à partir d'une adresse e-mail vérifiée sur le même domaine. Si vous configurez DKIM pour un domaine, tous les messages que vous envoyez à partir de ce domaine sont signés par DKIM, sauf pour les adresses e-mail que vous avez vérifiées individuellement. Les adresse e-mail vérifiées individuellement utilisent des paramètres distincts. Par exemple, si vous avez configuré DKIM pour le domaine example.com, et que vous avez vérifié séparément l'adresse e-mail mary@example.com (mais que vous n'avez pas configuré DKIM pour l'adresse), les e-mails que vous envoyez à partir de mary@example.com sont envoyés sans authentification DKIM. Vous pouvez résoudre ce problème en supprimant l'identité de l'adresse e-mail de la liste des identités de votre compte.
- Si vous utilisez la même identité dans plusieurs régions AWS, vous devez configurer DKIM pour chaque région séparément. De même, si vous utilisez le même domaine avec plusieurs comptes AWS, vous devez configurer DKIM pour chaque compte. Si vous supprimez les enregistrements DNS nécessaires pour une région ou un compte spécifique, Amazon SES

désactive la signature DKIM dans ce compte ou cette région. Si la signature DKIM est désactivée, Amazon SES vous envoie une notification par e-mail.

La console Amazon SES présente les détails DKIM suivants pour votre domaine : DKIM: waiting on sender verification... État de la vérification DKIM : vérification en attente.

Si vous effectuez les procédures décrites dans Easy DKIM ou BYODKIM - Bring Your Own DKIM (Fournissez votre propre DKIM) pour configurer DKIM pour un domaine, mais que la console Amazon SES indique toujours que la vérification DKIM est en attente, procédez comme suit :

- Attendez jusqu'à 72 heures. Dans de rares cas, un certain temps peut s'écouler avant que les enregistrements DNS soient visibles dans Amazon SES.
- Vérifiez que le registre CNAME (pour Easy DKIM) ou le registre TXT (pour BYODKIM) utilise le nom correct. Certains fournisseurs DNS ajoutent automatiquement le nom de domaine aux enregistrements que vous créez. Par exemple, si vous créez un registre avec le nom `example._domainkey.example.com`, votre fournisseur DNS peut ajouter le nom de votre domaine à la fin de cette chaîne, ce qui donne `example._domainkey.example.com.example.com`. Pour plus d'informations, consultez la documentation de votre fournisseur DNS.

Vous recevez un e-mail de la part d'Amazon SES qui indique que votre configuration DKIM a été (ou sera) révoquée.

Cela signifie qu'Amazon SES ne peut plus trouver les enregistrements CNAME requis (si vous avez utilisé Easy DKIM) ou le registre TXT requis (si vous avez utilisé BYODKIM) sur votre serveur DNS. L'e-mail de notification vous informe du délai dont vous disposez pour republier les enregistrements DNS avant que la configuration DKIM n'ait le statut révoqué et que la signature DKIM soit désactivée. Si votre configuration DKIM est révoquée, vous devez reprendre la procédure de configuration DKIM depuis le début.

Lors de la tentative de configuration de BYODKIM, le processus de vérification DKIM échoue.

Assurez-vous que votre clé privée utilise le bon format. La clé privée doit être au format PKCS #1 ou PKCS #8 et utiliser le chiffrement RSA 1 024 bits ou 2 048 bits. En outre, la clé privée doit être encodée en base64.

Lors de la configuration de BYODKIM, vous recevez une erreur **`BadRequestException`** lorsque vous essayez de spécifier une clé publique pour le domaine.

Si vous recevez une erreur `BadRequestException`, procédez comme suit :

- Assurez-vous que le sélecteur que vous spécifiez pour la clé publique contient au moins 1 caractère alphanumérique et 63 caractères alphanumériques au maximum. Le sélecteur ne peut pas inclure de points, de symboles ou de signes de ponctuation.
- Assurez-vous d'avoir supprimé les lignes d'en-tête et de pied de page de la clé publique, ainsi que tous les sauts de ligne de la clé publique.

Lorsque vous utilisez Easy DKIM, vos serveurs DNS retournent avec succès les enregistrements CNAME Amazon SES DKIM, mais renvoient **`SERVFAIL`** pour le registre TXT de vérification de domaine.

> Il se peut que votre fournisseur DNS ne soit pas en mesure de rediriger les enregistrements CNAME. Amazon SES et les FAI interrogent les enregistrements TXT. Pour être conformes à la spécification DKIM, vos serveurs DNS doivent pouvoir répondre aux requêtes de registres TXT, ainsi qu'aux requêtes de registres CNAME. Si votre fournisseur DNS n'est pas en mesure de répondre aux requêtes de registre TXT, une alternative consiste à utiliser Route 53 comme fournisseur d'hébergement DNS.

Vos e-mails contiennent deux signatures DKIM

> La signature DKIM supplémentaire, qui contient `d=amazonses.com`, est automatiquement ajoutée par Amazon SES. Vous pouvez l'ignorer.

Problèmes de remise Amazon SES

Une fois que votre demande à Amazon SES a abouti, votre message est souvent envoyé immédiatement. Dans d'autres cas, un léger retard peut être observé. Dans tous les cas, vous pouvez être assuré que votre e-mail sera envoyé.

Toutefois, lorsqu'Amazon SES envoie votre message, sa remise peut être contrariée par plusieurs facteurs, et dans certains cas, vous ne prendrez conscience que la remise a échoué en constatant que le message envoyé n'est pas arrivé à destination. Pour résoudre ce problème, procédez comme indiqué ci-dessous.

Si un e-mail n'arrive pas à destination, essayez la solution suivante :

- Vérifiez que vous avez formulé une demande `SendEmail` ou `SendRawEmail` pour l'e-mail en question et que vous avez reçu une réponse positive. Si vous formulez ces demandes par programmation, consultez les journaux de votre logiciel pour vérifier que le programme a bien effectué la demande et qu'il a reçu une réponse positive.

- Lisez l'article de blog Three places where your email could get delayed when sending through SES, car il peut s'agir en réalité d'un problème de retard et non d'un échec de la remise.
- Vérifiez la validité de l'adresse e-mail de l'expéditeur (adresse d'expédition). De même, vérifiez l'adresse de retour, qui est l'adresse où sont envoyés les messages retournés à l'expéditeur. Si votre e-mail est retourné à l'expéditeur, vous y trouverez un message d'erreur explicatif.
- Consultez AWS Service Health Dashboard pour vérifier qu'un problème connu n'affecte pas Amazon SES.
- Contactez le destinataire de l'e-mail ou le FAI du destinataire. Vérifiez que le destinataire utilise la bonne adresse e-mail et que son FAI ne fait face à aucun problème de remise connu. De même, déterminez si l'e-mail n'a pas été filtré comme courrier indésirable après être arrivé à destination.
- Si vous avez souscrit un Plan AWS Support payant, vous pouvez ouvrir une nouvelle demande de support technique. Dans la correspondance que vous nous adressez, indiquez les adresses de destinataires appropriées, ainsi que les ID de demande ou les ID de message renvoyés dans les réponses de `SendEmail` ou `SendRawEmail`.
- Attendez de voir si le problème n'est pas en réalité un retard plutôt qu'un échec de remise permanent. Pour lutter contre les expéditeurs de courrier indésirable, certains FAI rejettent temporairement les messages entrants en provenance des serveurs de messagerie inconnus. Ce processus, appelé inscription sur liste grise (ou « greylisting »), peut occasionner des retards de remise. Amazon SES tentera à nouveau d'envoyer ces messages. Si l'inscription sur liste grise est à l'origine du problème, le FAI acceptera peut-être l'e-mail lors de l'une de ces nouvelles tentatives.
- Même lorsque vous avez l'intérêt de vos clients à l'esprit, vous pouvez être confronté à des situations qui ont un impact négatif sur la délivrabilité de vos messages. Consultez the section called “Conseils et bonnes pratiques” qui vous aidera à vous assurer que vos communications par e-mail atteignent le public visé.

Problèmes au niveau des e-mails reçus d'Amazon SES

Cette section traite de certains problèmes courants que vous pouvez voir lorsque vous recevez des e-mails qui ont été envoyés depuis Amazon SES.

Le client de messagerie affiche « envoyé via amazonses.com » comme source de l'e-mail

> Certains clients de messagerie affichent le domaine « via » lorsque le domaine de l'expéditeur ne correspond pas au domaine à partir duquel l'e-mail a été envoyé (dans ce cas, amazonses.com). Pour de plus amples informations, veuillez consulter Extra info next to sender's name sur le site

web du support Gmail. Vous pouvez également configurer standard DKIM (DomainKeys Identified Mail) (DKIM). Lorsque vous authentifiez vos e-mails à l'aide de DKIM, les clients de messagerie n'affichent généralement pas le domaine intermédiaire, car la signature DKIM montre que l'e-mail est issu du domaine dont il prétend provenir. Pour de plus amples informations sur la configuration de DKIM, veuillez consulter Authentification d'e-mails avec DKIM dans Amazon SES.

> **Note**
>
> Si vous avez reçu du courrier indésirable ou d'autres e-mails non sollicités de la part d'un utilisateur SES, utilisez les outils de signalement de courrier indésirable dans votre client de messagerie, et suivez les étapes pour signaler un e-mail malveillant SES, répertoriées sous Nous contacter.

Le message contient des caractères brouillés ou n'ayant aucun sens

Si votre message contient des caractères qui ne figurent pas dans le jeu de caractères ASCII (tels que des caractères latins accentués, des caractères chinois ou des caractères arabes), vous devez les encoder à l'aide de l'encodage de caractères HTML. Vous pouvez utiliser des outils web pour encoder les caractères de votre e-mail, tels que le convertisseur de caractères HTML sur le site web de messagerie On Acid.

Vous pouvez également composer le message MIME vous-même. Dans le message MIME, vous pouvez spécifier l'utilisation de l'encodage UTF-8 dans le message. Lorsque vous utilisez l'encodage UTF-8, vous pouvez utiliser des caractères non-ASCII directement dans vos messages. Une fois que vous avez créé le message MIME, vous pouvez l'envoyer à l'aide de l'API SendRawEmail ou de l'API SendMail v2.

Une cause fréquente de ce problème est la fonctionnalité Guillemets intelligents de Microsoft Word. Si vous copiez souvent du contenu à partir de Word et que vous le collez dans vos e-mails, vous risquez de rencontrer ce problème. La fonction Guillemets intelligents remplace les guillemets droits ("...") par des guillemets courbes (“...”). Les guillemets courbes ne sont pas des caractères ASCII standard. Par conséquent, ils peuvent être rendus dans certains clients de messagerie par les caractères « ?? » ou des groupes de caractères tels que « â€œ ». Pour corriger ce problème, vous pouvez désactiver la fonctionnalité Guillemets intelligents dans Word. Vous pouvez également utiliser la solution SendRawEmail du paragraphe précédent. Pour savoir comment désactiver cette fonctionnalité, veuillez consulter Guillemets intelligents dans Word sur le site web du support Microsoft Office.

Problèmes de notifications Amazon SES

Si vous rencontrez un problème de notifications de retour à l'expéditeur, de réclamation ou de message délivré, passez en revue les causes et les solutions possibles ci-dessous.

- Vous recevez des notifications de retour à l'expéditeur via Amazon SNS, mais vous ne savez pas à quels destinataires ces notifications correspondent – Dans l'avenir, pour associer une notification de retour à l'expéditeur à un destinataire donné, vous disposez des possibilités suivantes :
  - Dans la mesure où Amazon SES ne stocke pas les ID de messages personnalisés que vous avez ajoutés, stockez un mappage entre un identificateur et l'ID de message Amazon SES qui vous est transmis en retour au moment où Amazon SES accepte l'e-mail.
  - Dans chaque appel à Amazon SES, plutôt que d'envoyer un message unique à plusieurs destinataires, envoyez-le à un seul destinataire.
  - Vous pouvez activer le transfert de commentaires par e-mail, qui vous transfère l'intégralité du message de retour à l'expéditeur.
- Vous recevez des notifications de réclamation ou de livraison via Amazon SNS ou le transfert de commentaires par e-mail, mais vous ne savez pas à quels destinataires ces notifications correspondent – Certains ISP occultent l'adresse e-mail du destinataire à l'origine de la réclamation avant de transmettre la notification de réclamation à Amazon SES. Le meilleur moyen de trouver l'adresse e-mail du destinataire est de stocker votre propre mappage entre un identificateur et l'ID de message Amazon SES qui vous est transmis en retour au moment où Amazon SES accepte l'e-mail. Notez qu'Amazon SES ne stocke pas les ID de messages personnalisés que vous ajoutez.
- Vous souhaitez configurer les notifications de façon à les diriger vers une rubrique Amazon SNS dont vous n'êtes pas propriétaire – Le propriétaire de cette rubrique doit configurer une stratégie d'accès Amazon SNS qui autorise votre compte à appeler l'action `SNS:Publish` sur sa rubrique. Pour savoir comment contrôler l'accès à votre rubrique Amazon SNS par l'utilisation de stratégies IAM, consultez Gestion de l'accès à vos rubriques Amazon SNS dans le Guide du développeur Amazon Simple Notification Service.

Erreurs d'envoi d'e-mails Amazon SES

Cette rubrique passe en revue les types d'erreurs propres à l'envoi d'e-mails que vous pouvez rencontrer lorsque vous envoyez un e-mail via Amazon SES. Si vous essayez d'envoyer un e-mail via Amazon SES et que l'appel à Amazon SES échoue, Amazon SES renvoie un message d'erreur

à votre application et n'envoie pas l'e-mail. La façon dont s'affiche ce message d'erreur dépend de la façon dont vous appelez Amazon SES.

- Si vous appelez l'API Amazon SES directement, l'action de requête renvoie une erreur. L'erreur peut être `MessageRejected` ou l'une des erreurs spécifiées dans la rubrique Common Errors (Erreurs courantes) du document Amazon Simple Email Service API Reference.
- Si vous appelez Amazon SES à l'aide d'un kit de développement logiciel (SDK) AWS qui utilise un langage de programmation qui prend en charge les exceptions, Amazon SES peut lever une exception. Le type d'exception varie en fonction du kit SDK et de l'erreur. Par exemple, il peut s'agir d'une exception `MessageRejectedException` Amazon SES (le nom réel peut varier en fonction du kit SDK) ou d'une exception AWS générale. Quel que soit le type d'exception, le type d'erreur et le message d'erreur de l'exception fournissent un complément d'information.
- Si vous appelez Amazon SES via son interface SMTP, la façon dont l'erreur se manifeste dépend de l'application. Certaines applications peuvent afficher un message d'erreur spécifique, contrairement à d'autres. Pour obtenir la liste des codes de réponse SMTP Amazon SES renvoyés, veuillez consulter Codes de réponse SMTP renvoyés par Amazon SES.

> **Note**
>
> En cas d'échec de votre appel à Amazon SES pour l'envoi d'un e-mail, vous n'êtes pas facturé pour ce message.

Vous trouverez ci-dessous les types de problèmes propres à Amazon SES qui peuvent conduire Amazon SES à renvoyer une erreur lors de votre tentative d'envoi d'un e-mail. Ces erreurs s'ajoutent aux erreurs AWS générales comme `MalformedQueryString`, telles qu'indiquées dans la rubrique Common Errors (Erreurs courantes) du document Référence Amazon Simple Email Service API.

- L'adresse e-mail n'est pas vérifiée. Les identités suivantes n'ont pas pu être vérifiées dans la région région : identité1, identité2, identité3 – Vous essayez d'envoyer un message à partir d'une adresse e-mail ou d'un domaine que vous n'avez pas vérifié avec Amazon SES. Cette erreur peut s'appliquer à l'adresse d'expédition, à l'adresse source, à l'adresse de l'expéditeur ou à l'adresse de retour. Si votre compte est toujours dans l'environnement de test (sandbox) Amazon SES, vous devez également vérifier l'adresse e-mail de chaque destinataire, hormis ceux fournis par le simulateur de boîte aux lettres Amazon SES. Si Amazon SES ne peut pas afficher toutes les identités en échec, le message d'erreur se termine par des points de suspension.

> **Note**
>
> Amazon SES dispose de points de terminaison dans plusieurs Régions AWS, et le statut de vérification d'adresse e-mail est distinct pour chaque Région AWS. Vous devez mener à bien le processus de vérification pour chaque expéditeur de la ou des Régions AWS que vous souhaitez utiliser.

- Account is paused (Compte suspendu) – La capacité de votre compte à envoyer des e-mails est suspendue. Vous pouvez toujours accéder à la console Amazon SES et exécuter la plupart des opérations. Toutefois, si vous essayez d'envoyer un e-mail, vous recevez ce message.

  Lorsque nous suspendons la capacité d'un compte à envoyer des e-mails, nous envoyons automatiquement une notification à l'adresse e-mail associée au Compte AWS. Pour de plus amples informations, veuillez consulter . the section called “FAQ sur le processus de vérification des envois”.
- Throttling (Limitation) – Il se peut que votre application tente d'envoyer des messages en trop grande quantité par seconde ou il se peut que vous ayez envoyé des e-mails en trop grande quantité au cours des dernières 24 heures. Dans ces cas, le message d'erreur peut être similaire aux exemples suivants :
  - Daily message quota exceeded (Quota de messages quotidien dépassé) – Vous avez envoyé le nombre maximum de messages autorisé sur une période de 24 heures. Si vous avez dépassé votre quota journalier, vous devez attendre la prochaine période de 24 heures avant de pouvoir envoyer plus d'e-mails.
  - Maximum sending rate exceeded (Taux d'envoi maximum dépassé) – Vous essayez d'envoyer plus d'e-mails par seconde que votre taux d'envoi maximum vous le permet. Si vous avez dépassé votre taux d'envoi, vous pouvez continuer d'envoyer des e-mails, mais vous devez réduire votre taux d'envoi. Pour en savoir plus, consultez Comment traiter l'erreur « Throttling - Maximum sending rate exceeded » (Restriction - Taux d'envoi maximum dépassé) ? sur le blog AWS Messaging and Targeting (Messagerie et ciblage).
  - Maximum SigV2 SMTP sending rate exceeded (Fréquence d'envoi maximale de SMTP SigV2 dépassée) – Vous tentez d'envoyer des messages à l'aide d'informations d'identification SMTP créées avant le 10 janvier 2019 ; vos informations d'identification SMTP ont été créées à l'aide d'une version antérieure d'AWS Signature. Pour des raisons de sécurité, vous devez supprimer les informations d'identification que vous avez créées avant cette date et les remplacer par de nouvelles informations d'identification. Vous pouvez supprimer d'anciennes informations

d'identification à l'aide de la console IAM. Pour plus d'informations sur la création d'informations d'identification, consultez the section called “Obtention des informations d'identification SMTP”.

Vous avez tout intérêt à surveiller régulièrement votre activité d'envoi pour vous situer par rapport à vos quotas d'envoi. Pour de plus amples informations, veuillez consulter . Surveillance de vos quotas d'envoi Amazon SES. Pour obtenir des informations générales sur les quotas d'envoi, consultez Gestion de vos limites d'envoi Amazon SES. Pour savoir comment accroître vos quotas d'envoi, consultez Augmentation de vos quotas d'envoi Amazon SES.

> **Important**
>
> Si le texte de l'erreur expliquant l'erreur de limitation n'a aucun rapport avec le dépassement de votre quota journalier ou de votre taux d'envoi maximum, il se peut qu'un problème à l'échelle du système soit à l'origine d'une réduction des capacités d'envoi. Pour obtenir des informations sur l'état du service, accédez à AWS Service Health Dashboard.

- There are no recipients specified (Aucun destinataire n'est spécifié) – Aucun destinataire n'a été indiqué.
- There are non-ASCII characters in the email address (L'adresse e-mail comporte des caractères non ASCII) – L'adresse e-mail doit être une chaîne ASCII de 7 bits. Si vous souhaitez effectuer un envoi vers ou à partir d'adresses e-mail qui contiennent des caractères Unicode dans la partie domaine de l'adresse, vous devez encoder le domaine à l'aide de Punycode. La syntaxe Punycode n'est pas autorisée dans la partie locale de l'adresse e-mail (c'est-à-dire, la partie qui précède le signe @) ni dans le « nom d'expéditeur convivial ». Si vous souhaitez utiliser des caractères Unicode dans le « nom d'expéditeur convivial », vous devez l'encoder en employant une syntaxe de mots encodés MIME, comme indiqué dans Envoi d'e-mails bruts à l'aide de l'API Amazon SES v2. Pour en savoir plus sur Punycode, consultez RFC 3492.
- Mail FROM domain is not verified (Le domaine MAIL FROM n'est pas vérifié) – Amazon SES n'a pas pu lire le registre MX nécessaire à l'utilisation du domaine MAIL FROM spécifié. Pour plus d'informations sur la configuration de domaines MAIL FROM personnalisés, consultez Utilisation d'un domaine MAIL FROM personnalisé.
- Configuration set does not exist (Le jeu de configurations n'existe pas) – Le jeu de configurations que vous avez spécifié n'existe pas. Un jeu de configurations est un paramètre facultatif qui permet de publier des événements d'envoi d'e-mails. Pour de plus amples informations, veuillez consulter . Surveillance de l'envoi d'e-mails à l'aide de la publication d'événements Amazon SES.

Accroissement du débit avec Amazon SES

Lorsque vous envoyez des e-mails, vous pouvez appeler Amazon SES aussi souvent que votre taux d'envoi maximum vous l'autorise. (Pour en savoir plus sur votre taux d'envoi maximum, consultez Gestion de vos limites d'envoi Amazon SES.) Cependant, chaque appel à Amazon SES demande un certain temps avant d'aboutir.

Si vous formulez plusieurs appels à Amazon SES à partir de l'API Amazon SES ou de l'interface SMTP, tenez compte des conseils suivants pour améliorer votre débit :

- Mesurez vos performances actuelles pour identifier les goulots d'étranglement – Pour tester vos performances, vous pouvez envoyer plusieurs e-mails de test le plus rapidement possible dans une boucle de code au sein de votre application. Mesurez la latence du cycle aller-retour de chaque demande `SendEmail`. Lancez ensuite de façon incrémentielle des instances supplémentaires de l'application sur la même machine, puis observez-en l'impact sur la latence du réseau. Vous pouvez également exécuter ce test sur plusieurs machines et sur différents réseaux pour mieux repérer les éventuels goulots d'étranglement au niveau des ressources des machines ou des réseaux.
- (API uniquement) Envisagez d'utiliser des connexions HTTP persistantes – Au lieu de vous contraindre à mettre en place une nouvelle connexion HTTP distincte pour chaque demande API, utilisez des connexions HTTP persistantes. En somme, cela consiste à réutiliser une même connexion pour plusieurs demandes d'API.
- Envisagez d'utiliser plusieurs threads – Lorsqu'une application utilise un seul thread, le code de l'application appelle l'API Amazon SES et attend de façon synchrone une réponse de l'API. L'envoi d'e-mails étant généralement une opération liée aux I/O, le recours à plusieurs threads offre un meilleur débit. Vous pouvez effectuer un envoi simultané en utilisant autant de threads d'exécution que vous le souhaitez.
- Envisagez d'utiliser plusieurs processus – L'utilisation de plusieurs processus peut vous aider à accroître votre débit, car vous aurez davantage de connexions actives simultanées à Amazon SES. Par exemple, vous pouvez segmenter les e-mails prévus en plusieurs compartiments, puis exécuter simultanément plusieurs instances de votre script d'envoi d'e-mails.
- Envisagez d'utiliser un relais de messagerie local – Votre application peut rapidement transmettre les messages à votre serveur de messagerie local, ce qui facilite leur mise en mémoire tampon et leur transmission asynchrone à Amazon SES. Certains serveurs de messagerie prennent en charge les remises simultanées, ce qui signifie que même si votre application génère des e-mails à destination du serveur de messagerie dans une opération à thread unique, le serveur

de messagerie utilise plusieurs threads lors de l'envoi vers Amazon SES. Pour de plus amples informations, veuillez consulter Intégration d'Amazon SES à votre serveur de messagerie existant.

- Envisagez d'héberger votre application plus près du point de terminaison de l'API Amazon SES – Il se peut que vous envisagiez d'héberger votre application dans un centre de données proche du point de terminaison de l'API Amazon SES ou sur une instance EC2 Amazon dans la même région AWS que le point de terminaison de l'API Amazon SES. Cela peut contribuer à diminuer la latence réseau entre votre application et Amazon SES, et à améliorer le débit. Pour connaître la liste des régions dans lesquelles Amazon SES est disponible, consultez Amazon Simple Email Service (Amazon SES) dans le document Références générales AWS.
- Envisagez d'utiliser plusieurs machines – Selon la configuration système de votre machine hôte, vous pouvez être limité par le nombre de connexions HTTP simultanées vers une seule adresse IP, ce qui peut limiter les avantages du parallélisme dès lors que vous dépassez un certain nombre de connexions simultanées sur une même machine. S'il s'agit d'un goulot d'étranglement, vous pouvez envisager de formuler des demandes Amazon SES simultanées en utilisant plusieurs machines.
- Envisagez d'utiliser l'API de requête à la place du point de terminaison SMTP – En utilisant l'API de requête Amazon SES, vous pouvez soumettre la demande d'envoi d'e-mails dans un seul et même appel réseau, alors que l'interfaçage avec le point de terminaison SMTP implique une conversation SMTP qui consiste en plusieurs demandes réseau (par exemple, EHLO, MAIL FROM, RCPT TO, DATA, QUIT). Pour en savoir plus sur l'API de requête Amazon SES, consultez Utilisation de l'API Amazon SES pour envoyer un e-mail.
- Utilisez le simulateur de boîte aux lettres (mailbox) Amazon SES pour tester votre débit maximum – Pour tester les modifications que vous souhaitez éventuellement mettre en œuvre, vous pouvez utiliser le simulateur de boîte aux lettres (mailbox). Il peut en effet vous aider à déterminer le débit maximal de votre système sans épuiser votre quota d'envoi quotidien. Pour obtenir des informations sur le simulateur de boîte aux lettres e-mail (mailbox), consultez Utilisation manuelle du simulateur de boîte aux lettres.

Si vous accédez à Amazon SES par le biais de son interface SMTP, consultez Problèmes SMTP Amazon SES pour prendre connaissance des problèmes spécifiques propres à SMTP qui peuvent avoir des répercussions sur le débit.

Problèmes SMTP Amazon SES

Cette section contient des solutions pour plusieurs problèmes courants liés à l'envoi d'e-mails via l'interface Amazon SES SMTP (Simple Mail Transfer Protocol). Il contient également une liste de codes de réponse SMTP qu'Amazon SES renvoie.

Pour en savoir plus sur l'envoi d'e-mails via l'interface Amazon SES SMTP, veuillez consulter Utilisation de l'interface SMTP d'Amazon SES pour envoyer des e-mails.

- Vous ne pouvez pas vous connecter au point de terminaison SMTP Amazon SES.

  Les problèmes de connexion au point de terminaison SMTP Amazon SES sont généralement imputables aux aléas suivants :

  - Informations d'identification incorrectes — Les informations d'identification que vous utilisez pour vous connecter au point de terminaison SMTP sont différentes de vos AWS informations d'identification. Pour obtenir vos informations d'identification SMTP, consultez Obtention des informations d'identification SMTP Amazon SES. Pour en savoir plus sur les informations d'identification, consultez Types d'informations d'identification Amazon SES.
  - Problèmes de réseau ou de pare-feu – Il est possible que votre réseau bloque les connexions sortantes sur le port à partir duquel vous essayez d'envoyer des e-mails. Pour déterminer si les problèmes de connexion sont liés à votre réseau local, entrez la commande suivante sur ligne de commande en remplaçant *`port`* par le port que vous essayez d'utiliser (en général, 465, 587, 2465 ou 2587) : `telnet email-smtp.us-west-2.amazonaws.com` *`port`*

    Si vous parvenez à vous connecter au serveur SMTP en utilisant cette commande et que vous essayez de vous connecter à Amazon SES en utilisant TLS Wrapper ou STARTTLS, suivez les procédures décrites dans Test de votre connexion à l'interface SMTP Amazon SES à l'aide de la ligne de commande.

    Si vous ne parvenez pas à vous connecter au point de terminaison SMTP Amazon SES en utilisant `telnet` ou `openssl`, cela indique que quelque chose dans votre réseau (un pare-feu, par exemple) bloque les connexions sortantes sur le port que vous essayez d'utiliser. Rapprochez-vous de votre administrateur réseau pour effectuer un diagnostic et corriger le problème.
- Vous envoyez à Amazon SES à partir d'une instance EC2 Amazon en utilisant le port 25, et vous recevez des expirations de délai d'attente.

  Amazon EC2 restreint le port 25 par défaut. Pour supprimer ces restrictions, envoyez une demande Amazon EC2 de suppression des limites d'envoi d'e-mails. Vous pouvez également vous connecter à Amazon SES à l'aide des ports 465 ou 587, aucun des deux n'étant limité.
- Des erreurs réseau provoquent des abandons d'e-mails.

  Vérifiez que votre application utilise la logique de relance lorsqu'elle se connecte au point de terminaison SMTP Amazon SES, et qu'elle est en mesure de détecter les erreurs réseau et, le

cas échéant, de tenter à nouveau la remise des messages. SMTP est un protocole détaillé et l'envoi d'un e-mail avec ce protocole exige plusieurs allers et retours réseau. La nature de SMTP augmente les risques d'erreurs réseau.

- Vous perdez la connexion avec le point de terminaison SMTP.

  Les connexions perdues sont le plus souvent causées par les problèmes suivants :

  - Taille MTU – Si vous recevez un message d'erreur lié à un dépassement de délai, il se peut que l'unité de transmission maximale (MTU) de l'interface réseau de l'ordinateur que vous utilisez pour vous connecter à l'interface SMTP Amazon SES soit trop importante. Pour résoudre ce problème, définissez une taille MTU de 1 500 octets sur cet ordinateur.

    Pour en savoir plus sur la définition de la taille MTU sur les systèmes d'exploitation Windows, Linux et macOS, consultez Des requêtes semblent se bloquer et parfois échouent à atteindre le cluster dans le guide de gestion Amazon Redshift.

    Pour plus d'informations sur la définition de la taille de la MTU pour une instance Amazon EC2, consultez la section Unité de transmission maximale (MTU) du Network Maximum Transmission Unit (MTU) pour votre instance EC2 dans le guide de l'utilisateur Amazon EC2.

  - Connexions à longue durée de vie – Le point de terminaison SMTP Amazon SES s'exécute sur une flotte d'instances Amazon EC2 derrière un Elastic Load Balancer (ELB). Afin de garantir que le système est tolérant up-to-date aux pannes, les instances Amazon EC2 actives sont régulièrement résiliées et remplacées par de nouvelles instances. Dans la mesure où votre application se connecte à une instance via l'ELB, la connexion devient non valide dès lors que l'instance EC2 Amazon est résiliée. Vous devez établir une nouvelle connexion SMTP après avoir remis un nombre fixe de messages via une même connexion SMTP, ou si la connexion SMTP est active depuis un certain temps. Vous devrez effectuer des tests pour trouver les seuils adaptés à votre application, selon l'endroit où elle est hébergée et la façon dont elle envoie les e-mails à Amazon SES.

- Vous souhaitez connaître les adresses IP des serveurs de messagerie SMTP Amazon SES de façon à pouvoir ajouter ces adresses à la liste autorisée de votre réseau.

  Les adresses IP des points de terminaison SMTP Amazon SES résident derrière les équilibreurs de charge. Par conséquent, ces adresses IP changent fréquemment. Il n'est pas possible de fournir une liste définitive de toutes les adresses IP des points de terminaison Amazon SES. Nous vous recommandons d'ajouter à la liste autorisée le domaine `amazonses.com` plutôt que des adresses IP individuelles.

Codes de réponse SMTP renvoyés par Amazon SES

Cette rubrique contient la liste des codes de réponse que l'interface SMTP Amazon SES renvoie.

Vous devez relancer les demandes SMTP qui reçoivent des erreurs 400. Nous vous recommandons de mettre en place un système qui retente les demandes avec des délais d'attente progressivement plus longs (par exemple, attendre 5 secondes avant de recommencer, puis 10 secondes, et enfin 30 secondes). Si la troisième relance n'aboutit pas, attendez 20 minutes, puis répétez le processus. Pour voir un exemple d'implémentation qui fait appel à une stratégie de relance exponentielle, consultez How to handle a « Throttling – Maximum sending rate exceeded » error (Comment traiter l'erreur « Restriction - taux d'envoi maximum dépassé » ?) sur le blog AWS Messaging and Targeting (Messagerie et ciblage) .

> **Note**
>
> AWS Les SDK implémentent automatiquement la logique de nouvelle tentative, mais ils utilisent l'interface HTTPS au lieu du protocole SMTP.

Si vous recevez une erreur 500, vous devez réviser la demande pour corriger le problème avant de soumettre à nouveau la demande. Par exemple, si vos informations AWS d'authentification ne sont pas valides, vous devez mettre à jour votre application pour utiliser les informations d'identification correctes avant de soumettre à nouveau votre demande.

Description	Code de réponse	En savoir plus
Authentification réussie	`235 Authentication successful`	Votre client SMTP s'est correctement connecté au serveur SMTP.
Remise réussie	`250 Ok` *`MessageID`*	*`MessageID`* est une chaîne de caractères unique dont se sert Amazon SES pour identifier un message.
Service non disponible	`421 Too many concurrent SMTP connections`	Amazon SES ne peut pas traiter la demande, car il y a actuellem

Description	Code de réponse	En savoir plus
		ent un trop grand nombre de connexions au serveur SMTP.
Erreur de traitement local	`451 Temporary service failure`	Amazon SES n'a pas pu traiter la demande. Il peut exister des problèmes avec la demande qui empêche son traitement.
Expiration	`451 Timeout waiting for data from client`	Trop de temps s'est écoulé entre les demandes. Le serveur SMTP a donc mis fin à la connexion.
Quota d'envoi quotidien dépassé	`454 Throttling failure: Daily message quota exceeded`	Vous avez dépassé le nombre maximum d'e-mails qu'Amazon SES vous permet d'envoyer en 24 heures. Pour plus d'informations, consultez Gestion de vos limites d'envoi Amazon SES.
Taux d'envoi maximum dépassé	`454 Throttling failure: Maximum sending rate exceeded`	Vous avez dépassé le nombre maximum d'e-mails qu'Amazon SES vous permet d'envoyer par seconde. Pour plus d'informations, consultez Gestion de vos limites d'envoi Amazon SES.

Description	Code de réponse	En savoir plus
Problème Amazon SES lors de la validation d'informations d'identification SMTP	`454 Temporary authentication failure`	Les problèmes pouvant entraîner ce dysfonctionnement incluent (sans s'y limiter) : • L'existence d'un problème de chiffrement entre votre application d'envoi d'e-mails et Amazon SES. Notez que vous devez utiliser une connexion chiffrée au moment de vous connecter à Amazon SES. Pour plus d'informations, consultez Connexion à un point de terminaison SMTP Amazon SES. • Il se peut qu'Amazon SES soit confronté à un problème. Vérifiez AWS Service Health Dashboard pour les mises à jour.
Problème de réception de la demande	`454 Temporary service failure`	Amazon SES n'a pas reçu la demande. En conséquence, le message n'a pas été envoyé.
Informations d'identification incorrectes	`530 Authentication required`	Votre application d'envoi d'e-mails n'a pas essayé de s'authentifier auprès d'Amazon SES lors de sa tentative de connexion à l'interface SMTP.

Description	Code de réponse	En savoir plus
Informations d'authentification non valides	`535 Authentication Credentials Invalid`	Votre application d'envoi d'e-mails n'a pas fourni les informations d'identification SMTP correctes à Amazon SES. Notez que vos informations d'identification SMTP ne sont pas les mêmes que vos AWS informations d'identification. Pour plus d'informations, consultez Obtention des informations d'identification SMTP Amazon SES.
Compte non abonné à Amazon SES	`535 Account not subscribed to SES`	Le propriétaire Compte AWS des informations d'identification SMTP n'est pas inscrit à Amazon SES.
Le message est trop long	`552 Message is too long.`	Le message que vous essayez d'envoyer a un poids supérieur à la taille maximale du message.
Compte non abonné à Amazon SES	`535 Account not subscribed to SES`	Le propriétaire Compte AWS des informations d'identification SMTP n'est pas inscrit à Amazon SES.
Erreur de syntaxe MAIL FROM	`553 <email-address > Invalid email address`	Une erreur de syntaxe se produit dans la partie MAIL FROM du message SMTP. Veuillez vérifier que vous suivez le bon format et que vous avez pensé à insérer l'adresse e-mail entre « **<>** ».

Description	Code de réponse	En savoir plus
Erreur de syntaxe RCPT TO	`553 <email-address > address unknown`	La partie RCPT TO du message SMTP contient une erreur de syntaxe. Veuillez vérifier que vous suivez le bon format et que vous avez pensé à insérer l'adresse e-mail entre « **<>** ».
Utilisateur non autorisé à appeler le point de terminaison SMTP Amazon SES	`554 Access denied: User UserARN is not authorized to perform ses:SendRawEmail on resource IdentityARN`	La politique AWS Identity and Access Management (IAM) ou la politique d'autorisation d'envoi Amazon SES de l'utilisateur propriétaire des informations d'identification SMTP n'est pas autorisé à appeler le point de terminaison SMTP Amazon SES.

Description	Code de réponse	En savoir plus
Adresse e-mail non vérifiée	`554 Message rejected: Email address is not verified. The following identities failed the check in region region: identity0 , identity1 , identity2`	Vous essayez d'envoyer un e-mail à partir d'une adresse e-mail ou d'un domaine qui ne sont pas vérifiés pour l'envoi d'e-mails à partir de votre compte Amazon SES. Cette erreur peut s'appliquer aux adresses « De », « Source », « Expéditeur » ou « Return-Path ». Si votre compte est toujours dans l'environnement de test (sandbox), vous devez également vérifier l'adresse e-mail de chaque destinataire, hormis ceux fournis par le simulateur de boîte aux lettres Amazon SES. Si Amazon SES n'est pas en mesure d'afficher toutes les identités ayant échoué au contrôle de vérification, le message d'erreur se termine par trois points (...). **Note** Amazon SES possède plusieurs points de terminaison Régions AWS, et le statut de vérification de l'adresse e-mail est distinct pour chacun Région AWS d'entre eux. Vous devez terminer le processus de vérification pour

Description	Code de réponse	En savoir plus
		chaque expéditeur Régions AWS que vous souhaitez utiliser.

> **Note**
>
> Pour les problèmes SMTP qui ne sont pas pris en charge par les procédures de résolution des problèmes présentées sur cette page, essayez les options de support SES répertoriées sous Nous contacter.

Questions fréquentes sur Amazon SES (FAQ)

Cette section contient les réponses aux questions fréquentes liées à l'utilisation d'Amazon SES.

Cette section contient les FAQ sur les rubriques suivantes :

- FAQ sur le processus de vérification des envois Amazon SES
- FAQ sur les listes DNSBL (DNS Blackhole Lists)
- FAQ sur les métriques Amazon SES d'envoi d'e-mails

FAQ sur le processus de vérification des envois Amazon SES

Nous contrôlons les e-mails envoyés via Amazon SES pour nous assurer que le service n'est pas utilisé pour envoyer des e-mails malveillants, indésirables ou de mauvaise qualité. Si nous déterminons qu'un utilisateur envoie un contenu qui entre dans l'une de ces catégories, nous exécutons des actions sur ce compte. Il s'agit de notre processus de vérification des envois.

Dans de nombreux cas, lorsque nous détectons un problème lié à un compte, nous plaçons ce compte sous vérification. Dans d'autres cas, nous suspendons la capacité du compte à envoyer des e-mails. Nous prenons ces mesures pour protéger la réputation de l'expéditeur de chaque compte et pour empêcher les autres utilisateurs de SES de connaître des interruptions de service et des problèmes de délivrabilité.

Table des matières

FAQ sur les comptes sous vérification

Q1. J'ai reçu un message indiquant que mon compte est sous vérification. Qu'est-ce que cela signifie ?

Nous avons détecté un problème avec les emails envoyés depuis votre compte et nous vous accordons du temps pour y remédier. Vous pouvez continuer à envoyer des e-mails comme vous le feriez normalement, mais vous devez également résoudre le problème qui a provoqué le placement de votre compte sous vérification. Si vous ne corrigez pas le problème avant la fin de la période de vérification, nous pouvons suspendre votre capacité à envoyer d'autres e-mails.

Q2. Serai-je toujours informé si mon compte est placé sous vérification ?

Oui. Vous recevez une notification à l'adresse e-mail associée à votre compte AWS .

Q3. Pourquoi n'ai-je pas reçu une notification indiquant que mon compte est sous vérification ?

Lorsque votre compte est examiné, nous envoyons automatiquement une notification à l'adresse e-mail associée à votre AWS compte. Cette adresse e-mail est celle que vous avez spécifiée lors de la création de votre AWS compte. Dans certains cas, cette adresse e-mail peut être différente de celle que vous utilisez pour envoyer des e-mails via SES.

Nous vous recommandons de surveiller la réputation d'expéditeur en consultant régulièrement les Métriques de réputation. Vous pouvez également configurer des alarmes automatisées sur Amazon CloudWatch. Ces alarmes peuvent vous envoyer une notification lorsque vos métriques de réputation dépassent certains seuils. Vous pouvez également configurer Amazon CloudWatch pour qu'il vous contacte par d'autres moyens, par exemple en envoyant un SMS sur votre téléphone portable.

Q4. Le fait que mon compte SES soit en cours de révision aura-t-il un impact sur mon utilisation d'autres AWS services ?

Vous pourrez toujours utiliser d'autres AWS services pendant que votre compte SES est en cours de révision. Toutefois, si vous demandez une augmentation du quota de service pour un autre AWS service qui envoie des communications sortantes (tel qu'Amazon SNS), cette demande peut être refusée jusqu'à ce que la période de révision de votre compte SES soit levée.

Q5. Que dois-je faire si mon compte est sous vérification ?

Vous devez faire ce qui suit :

- Si votre situation le permet, arrêtez d'envoyer des e-mails jusqu'à ce que vous ayez résolu le problème. Vous aurez toujours la possibilité d'envoyer des e-mails pendant que votre compte est sous vérification. Toutefois, si vous continuez à envoyer des messages sans procéder à des modifications, vous risquer d'aggraver le problème sans le vouloir.
- Lisez l'e-mail que nous vous avons envoyé pour consulter un résumé du problème.
- Enquêtez sur votre envoi pour déterminer quel aspect de votre envoi a déclenché le problème.
- Après avoir apporté les modifications qui, selon vous, résoudront le problème, connectez-vous à la AWS console et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Dans le message, fournissez des informations détaillées sur les étapes que vous avez effectuées pour résoudre le problème et décrivez la manière dont ces étapes empêchent le problème de se reproduire.
- Veillez à fournir toutes les informations que nous demandons explicitement. Nous avons besoin de ces informations pour évaluer votre cas.

Q6. Comment demander un réexamen ?

Vous pouvez demander que nous revoyions notre décision de réexaminer votre compte. Pour demander un avis, connectez-vous à la AWS console et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom.

Dans la demande, fournissez les informations suivantes :

- Informations sur la cause principale de l'événement ayant entraîné le placement sous vérification de votre compte.
- La liste des modifications que vous avez effectuées pour corriger le problème. Incluez uniquement les étapes que vous avez déjà implémentées, et non celles que vous envisagez de mettre en œuvre à l'avenir.
- Informations indiquant comment ces modifications empêchent le même problème de se reproduire.

Selon la nature de l'événement qui nous a amenés à placer votre compte sous vérification, nous pouvons être amenés à demander des informations supplémentaires. Consultez la rubrique FAQ associée au problème que vous rencontrez pour obtenir une liste des informations à inclure dans votre demande.

Q7. Pourquoi ma demande de réexamen n'est-elle pas acceptée ?

Nous répondrons à votre demande avec des informations sur la raison pour laquelle nous n'avons pas accepté celle-ci. Dans certains cas, vous pourrez envoyer une autre demande si vous êtes en mesure de démontrer que vous avez résolu le problème et que vos modifications empêchent le problème de se reproduire.

Q8. Pouvez-vous m'aider à diagnostiquer le problème ?

En général, nous pouvons vous donner uniquement une idée générale de votre problème (par exemple, nous pouvons vous dire que vous avez un problème avec les retours à l'expéditeur). Vous devrez enquêter sur la cause profonde de votre côté.

Q9. Comment savoir si mon compte n'est plus sous vérification ?

Les métriques de réputation comprennent des informations concernant le statut actuel de votre compte. Pour plus d’informations, consultez Utilisation de métriques de réputation pour suivre les taux de retours à l'expéditeur et de réclamations..

Q10. Placez-vous mon compte sous vérification chaque fois qu'un problème a lieu ?

Non. Dans certains cas, nous pouvons suspendre la capacité de votre compte à envoyer des e-mails sans d'abord placer celui-ci sous vérification. Par exemple :

- Si le problème est très grave.
- Si votre compte a été placé sous vérification pour le même problème plusieurs fois par le passé. C'est pourquoi il est important de résoudre le problème sous-jacent plutôt que seulement résoudre l'incident spécifique à l'origine du placement sous vérification de votre compte. Par exemple, si une campagne spécifique nous a amenés à placer votre compte sous vérification, vous devez faire plus que seulement arrêter cette campagne. Vous devez déterminer quelles propriétés de la campagne ont été problématiques et vous assurer que vous disposez des processus en place pour que vos futures campagnes ne rencontrent pas le même problème.

Dans l'une ou l'autre de ces situations, nous vous envoyons automatiquement une notification lorsque nous suspendons la capacité de votre compte à envoyer des e-mails.

Q11. Que se passe-t-il si j'apporte mes corrections peu avant l'expiration de la période de vérification ?

Connectez-vous au AWS Management Console et rendez-vous dans le Centre de support. Répondez au cas que nous avons ouvert en votre nom. Dans votre réponse au cas, indiquez-nous que vous avez résolu le problème.

Q12. Puis-je obtenir de l'aide auprès de mon AWS représentant ou du Support Premium ?

Si vous travaillez déjà avec un AWS responsable du compte, nous le contacterons automatiquement lorsque votre compte sera examiné. Votre représentant peut être en mesure de fournir des informations supplémentaires afin de vous aider à mieux comprendre le problème. Si vous utilisez Premium Support, vous devez également contacter l'équipe pour obtenir une aide supplémentaire.

FAQ sur les suspensions d'envoi

Q1. J'ai reçu un message indiquant que la capacité de mon compte à envoyer des e-mails est suspendue. Qu'est-ce que cela signifie ?

Nous avons suspendu la capacité de votre compte à envoyer des e-mails en raison d'un problème critique avec les e-mails que vous avez envoyés. Le plus souvent, nous suspendons des comptes pour l'une des raisons suivantes :

- Nous avons précédemment placé votre compte sous vérification. Les problèmes qui nous ont amenés à placer votre compte sous vérification n'a pas été corrigé avant la fin de la période de vérification. Nous avons donc suspendu la capacité de votre compte à envoyer des e-mails.
- Nous avons placé votre compte sous vérification plusieurs fois pour le même problème.
- Votre compte a envoyé un e-mail enfreignant les Conditions de service AWS. Si ces violations sont graves, nous pouvons suspendre la capacité de votre compte à envoyer des e-mails sans d'abord placer celui-ci sous vérification.

Q2. Serai-je systématiquement informé si la capacité de mon compte à envoyer des e-mails est suspendue ?

Oui. Vous recevez une notification à l'adresse e-mail associée à votre compte AWS .

Q3. La capacité de mon compte à envoyer des e-mails est suspendue. Pourquoi n'ai-je pas reçu de notification ?

Lorsque nous suspendons la capacité d'un compte à envoyer des e-mails, nous envoyons automatiquement une notification à l'adresse e-mail associée au compte.

> **Note**
>
> Lorsque vous créez votre AWS compte, vous devez fournir une adresse e-mail. Vous pouvez modifier cette adresse à tout moment. Pour plus d'informations sur la modification de l'adresse associée à votre AWS compte, consultez la section Gestion d'un AWS compte dans le guide de AWS Billing and Cost Management l'utilisateur.

Vous pouvez utiliser Amazon CloudWatch pour créer des alarmes qui vous informent lorsque vos taux de rebond et de plaintes sont trop élevés. La création d'une alarme est un bon moyen de recevoir le plus tôt possible une alerte des facteurs qui pourraient nous conduire à suspendre la capacité d'envoi d'e-mails de votre compte. Toutefois, il existe des facteurs autres que les retours à l'expéditeur et les réclamations qui peuvent nous amener à suspendre votre capacité d'envoi d'e-mails. Pour plus d'informations sur la création d'alarmes dans CloudWatch, consultezCréation d'alarmes de surveillance de réputation avec CloudWatch.

Vous pouvez également utiliser le Acount Dashboard (Tableau de bord du compte) pour déterminer l'état actuel de votre compte. Par exemple, si la capacité de votre compte à envoyer des e-mails est actuellement suspendue, la section Account status (Statut du compte) du tableau de bord du compte affiche le statut Paused (En pause). Si votre compte est en mesure d'envoyer des e-mails normalement, l'état affiché est Healthy (Sain).

Enfin, vous pouvez consulter le AWS Health Dashboard (PHD) à l'adresse https://phd.aws.amazon.com/ pour déterminer si la capacité de votre compte à envoyer des e-mails est actuellement suspendue. Lorsque nous suspendons la capacité d'un compte à envoyer des e-mails, nous ajoutons automatiquement un événement SES sending paused (Envoi SES suspendu) à la section Event log (Journal des événements) du PHD. L'événement SES sending paused (Envoi SES suspendu) a toujours le statut Closed (Fermé), que la capacité du compte à envoyer des e-mails soit suspendue ou pas. Le journal des événements inclut également une copie de l'e-mail que nous avons envoyé à l'adresse e-mail associée à votre AWS compte lorsque l'événement de pause d'envoi s'est produit.

Vous pouvez l'utiliser CloudWatch pour créer des alarmes qui vous alertent lorsque de nouveaux événements apparaissent sur votre Personal Health Dashboard. Pour plus d'informations, consultez la section Surveillance des AWS Health événements à l'aide d' CloudWatch événements dans le guide de AWS Health l'utilisateur.

Q4. La capacité de mon compte à envoyer des e-mails est suspendue. Cela a-t-il un impact sur ma capacité à utiliser d'autres AWS services ?

Vous pouvez toujours utiliser d'autres AWS services pendant que la capacité de votre compte à envoyer des e-mails est suspendue. Toutefois, si vous demandez une augmentation des quotas de service pour un autre service AWS qui envoie des communications sortantes (par exemple, Amazon SNS), cette demande pourrait être refusée jusqu'à ce que la capacité de votre compte à envoyer des e-mails soit restaurée.

Q5. Que dois-je faire si la capacité de mon compte à envoyer des e-mails est suspendue ?

Vous devez faire ce qui suit :

- Lisez l'e-mail que nous vous avons envoyé pour consulter un résumé du problème.
- Enquêtez sur votre envoi pour déterminer quel aspect de votre envoi a déclenché le problème.
- Après avoir apporté les modifications qui, selon vous, résoudront le problème, connectez-vous à la AWS console et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Dans le message, fournissez des informations détaillées sur les étapes que vous avez effectuées pour résoudre le problème et décrivez la manière dont ces étapes empêchent le problème de se reproduire.
- Veillez à fournir toutes les informations que nous demandons explicitement. Nous avons besoin de ces informations pour évaluer votre cas.

Q6. Qu'est-ce qu'une vérification ?

Vous pouvez demander que nous réexaminions notre décision de placer votre compte sous vérification. Consultez la question suivante Pour en savoir plus sur une demande de réexamen.

Q7. Comment demander un réexamen ?

Pour demander un avis, connectez-vous à la AWS console et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom.

Dans la demande, fournissez les informations suivantes :

- Informations relatives à l'origine du problème.
- La liste des modifications que vous avez effectuées pour corriger le problème. Incluez uniquement les étapes que vous avez déjà implémentées, et non celles que vous envisagez de mettre en œuvre à l'avenir.
- Informations indiquant comment ces modifications empêcheront le même problème de se reproduire.

Selon la nature de l'événement qui nous a amenés à suspendre la capacité d'envoi d'e-mails de votre compte., nous pouvons demander des informations supplémentaires. Consultez la rubrique FAQ associée au problème que vous rencontrez pour obtenir une liste des informations à inclure dans votre demande.

Q8. Que se passe-t-il si ma demande n'est pas acceptée ?

Nous répondrons à votre demande avec des informations sur la raison pour laquelle nous n'avons pas accepté celle-ci. Dans certains cas, vous pourrez envoyer une autre demande si vous êtes en mesure de démontrer que vous avez résolu le problème et que vos modifications empêchent le problème de se reproduire.

Q9. Pouvez-vous m'aider à diagnostiquer le problème ?

En général, nous pouvons vous donner uniquement une idée générale de votre problème (par exemple, nous pouvons vous dire que vous avez un problème avec les retours à l'expéditeur). Il vous incombe de corriger le problème.

Q10. Comment savoir si la capacité de mon compte à envoyer des e-mails a été restaurée ?

Les métriques de réputation comprennent des informations concernant le statut actuel de votre compte. Pour plus d’informations, consultez Utilisation de métriques de réputation pour suivre les taux de retours à l'expéditeur et de réclamations..

Q11. Puis-je obtenir de l'aide auprès de mon AWS représentant ou du Support Premium ?

Si vous travaillez déjà avec un responsable du AWS compte, nous le contacterons automatiquement si nous interrompons la capacité de votre compte à envoyer des e-mails. Votre représentant peut être

en mesure de fournir des informations supplémentaires afin de vous aider à mieux comprendre le problème. Si vous utilisez Premium Support, vous devez également contacter l'équipe pour obtenir une aide supplémentaire.

FAQ sur les retours à l'expéditeur

Q1. En quoi mes retours à l'expéditeur vous gênent-ils ?

Des taux de retour à l'expéditeur élevés sont souvent utilisés par des entités telles que les fournisseurs de messagerie et les organisations anti-courrier indésirable pour détecter les expéditeurs qui se livrent à de mauvaises pratiques d'envoi d'e-mails. Des taux de retour à l'expéditeur élevés peuvent entraîner l'envoi d'e-mails dans le dossier de courrier indésirable plutôt que dans la boîte de réception.

Q2. Que dois-je faire si je reçois une notification indiquant que mon compte est sous vérification ou que mes envois sont interrompus en raison de mon taux de retour à l'expéditeur ?

Identifiez la cause du problème, puis corrigez-la. Après avoir apporté les modifications qui, selon vous, résoudront le problème, connectez-vous à la AWS console et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Dans le message, fournissez des informations détaillées sur les étapes que vous avez effectuées pour résoudre le problème et décrivez la manière dont ces étapes empêchent le problème de se reproduire. Incluez également les informations suivantes :

- La méthode utilisée pour assurer le suivi de vos retours à l'expéditeur.
- Comment vous veillez à ce que les adresses e-mail des nouveaux destinataires soient valides avant l'envoi. Par exemple, les recommandations suivies dans Q11. Que puis-je faire pour limiter les retours à l'expéditeur ?.

Q3. Quels sont les types de retours à l'expéditeur comptabilisés dans le taux de retour ?

Votre taux de retour à l'expéditeur comprend uniquement les retours à l'expéditeur définitifs pour des domaines que vous n'avez pas vérifiés. Les retours à l'expéditeur définitifs sont des échecs de remise permanents, tels que « l'adresse n'existe pas ». Les échecs intermittents et temporaires, comme « boîte aux lettres pleine », ou les retours à l'expéditeur en raison d'adresses IP bloquées, ne sont pas pris en compte pour le calcul du taux de retour.

Q4. Divulguez-vous les taux de retour à l'expéditeur qui peuvent entraîner le placement de mon compte sous vérification ou la suspension des mes envois ?

Pour un résultat optimal, vous devez maintenir un taux de retour inférieur à 2 %. Les taux de retour à l'expéditeur supérieurs peuvent avoir un impact sur la remise de vos e-mails.

Si votre taux de retour est de 5 % ou plus, nous placerons votre compte sous vérification. Si votre taux de retour à l'expéditeur est de 10 % ou plus, nous pouvons suspendre la capacité de votre compte à envoyer d'autres e-mails tant que vous n'avez pas résolu le problème à l'origine de ce taux élevé.

Q5. Pendant quelle période de temps mon taux de retour est-il calculé ?

Nous ne calculons pas votre taux de retour en fonction d'une durée fixée, car différents expéditeurs envoient à des taux différents. À la place, nous examinons un volume représentatif, c'est-à-dire une quantité d'e-mails qui représentent vos pratiques d'envoi habituelles. Afin d'être équitable à la fois pour les expéditeurs de volumes élevés et faibles, le volume représentatif est différent pour chaque utilisateur et évolue avec les tendances d'envoi de l'utilisateur.

Q6. Puis-je calculer mon propre taux de rebond en utilisant les informations de la console SES ou de l' GetSendStatistics API ?

Non. Le taux retour à l'expéditeur est calculé à l'aide de volume représentatif (voir Q5. Pendant quelle période de temps mon taux de retour est-il calculé ?). En fonction de votre taux d'envoi, votre taux de rebond peut remonter plus loin dans le temps que celui de la console SES ou `GetSendStatistics` ne peut être récupéré. En outre, seuls les e-mails envoyés vers des domaines non vérifiés sont pris en compte dans le calcul de votre taux de retour. Toutefois, si vous surveillez régulièrement votre taux de retour à l'aide de ces méthodes, vous devriez toujours être en mesure de détecter les problèmes avant qu'ils atteignent des niveaux susceptibles de nous amener à placer votre compte sous vérification ou à suspendre la capacité d'envoi d'e-mails de votre compte.

Q7. Comment puis-je connaître les adresses électroniques qui ont été retournées ?

Examinez les notifications de rebond que SES vous envoie. L'adresse e-mail à laquelle SES transmet les notifications dépend de la manière dont vous avez envoyé les messages d'origine, comme décrit à l'adresseRéception des notifications Amazon SES par e-mail. Vous pouvez également configurer les notifications de retour à l'expéditeur via Amazon Simple Notification Service (Amazon SNS), comme décrit dans Configuration de notifications d'événement pour Amazon SES. Notez que la simple suppression des adresses retournées de votre liste sans aucune enquête supplémentaire

ne résoudra pas toujours le problème sous-jacent. Pour en savoir plus sur ce que vous pouvez faire pour réduire les retours à l'expéditeur, consultez Q11. Que puis-je faire pour limiter les retours à l'expéditeur ?.

Q8. Si je n'ai pas surveillé mes retours à l'expéditeur, pouvez-vous me donner une liste d'adresses qui ont refusées ?

Non, nous ne pouvons pas fournir de liste complète des adresses qui ont refusé. Vous êtes chargé de surveiller et de réagir aux retours à l'expéditeur de votre compte.

Q9. Comment dois-je gérer les retours à l'expéditeur ?

Vous devez supprimer les adresses retournées de votre liste de diffusion et arrêter immédiatement de les utiliser pour les envois. Si vous êtes un petit expéditeur, il peut être suffisant de surveiller les retours à l'expéditeur par e-mail et de supprimer manuellement les adresses retournées de votre liste de diffusion. Si votre volume est plus élevé, vous pouvez probablement configurer l'automatisation pour ce processus, soit en traitant par programme la boîte aux lettres dans laquelle vous recevez les retours à l'expéditeur, soit en configurant les notifications de retour à l'expéditeur via Amazon SNS. Pour plus d'informations, consultez Configuration de notifications d'événement pour Amazon SES.

Q10. Est-il possible que mes e-mails soient retournés parce que j'ai atteint mes quotas d'envoi ?

Non. Les retours à l'expéditeur ne sont pas liés aux quotas d'envoi. Si vous essayez de dépasser votre quota d'envoi, vous recevrez une erreur de l'API SES ou de l'interface SMTP lorsque vous tenterez d'envoyer un e-mail.

Q11. Que puis-je faire pour limiter les retours à l'expéditeur ?

Tout d'abord, assurez-vous que vous êtes conscient de vos retours à l'expéditeur (voir Q7. Comment puis-je connaître les adresses électroniques qui ont été retournées ?). Ensuite, suivez ces instructions :

- N'achetez pas, ne louez pas ou ne partagez pas d'adresses e-mail. Envoyez des e-mails uniquement aux destinataires qui ont explicitement demandé à en recevoir de votre part.
- Supprimez de votre liste les adresses e-mail correspondant à des retours à l'expéditeur.
- Sur les formulaires web, demandez aux utilisateurs d'entrer leurs adresses e-mail deux fois, et vérifiez que les deux adresses correspondent avant d'envoyer le formulaire.

- Utilisez la double acceptation pour inscrire de nouveaux utilisateurs. En d'autres termes, lorsque de nouveaux utilisateurs s'inscrivent, envoyez-leur un e-mail de confirmation sur lequel ils doivent cliquer avant de recevoir tout e-mail supplémentaire. Ceci évite que certaines personnes en inscrivent d'autres, ainsi que les inscriptions accidentelles.
- Si vous devez envoyer des messages à des adresses que vous n'avez pas contactées dernièrement (et, par conséquent, si vous ne pouvez pas être certain que les adresses sont toujours valides), faites-le uniquement avec une petite partie de votre envoi global. Pour en savoir plus, consultez notre article de blog Never send to old addresses, but what if you have to? (Vous ne devez jamais envoyer de messages à de vieilles adresses, mais que faire si vous devez le faire ?).
- Assurez-vous que vous ne structurez pas les inscriptions de façon à encourager les personnes à utiliser des adresses fictives. Par exemple, ne fournissez pas de valeur ajoutée ou d'avantages tant que les destinataires n'ont pas vérifié leurs adresses.
- Si vous avez une fonctionnalité d'envoi d'un e-mail à un ami, utilisez CAPTCHA ou un mécanisme similaire afin d'empêcher l'utilisation de la fonction automatisée, et n'autorisez pas les utilisateur à insérer de contenu arbitraire.
- Si vous utilisez SES pour les notifications du système, assurez-vous d'envoyer les notifications à de vraies adresses autorisées à recevoir du courrier. De même, n'oubliez pas de désactiver les notifications dont vous n'avez pas besoin.
- Si vous testez un nouveau système, assurez-vous que vous envoyez à des adresses réelles qui peuvent recevoir des e-mails ou que vous utilisez le simulateur de boîte aux lettres SES. Pour plus d'informations, consultez Utilisation manuelle du simulateur de boîte aux lettres.

FAQ sur les réclamations

Q1. Qu'est-ce qu'une réclamation ?

Une réclamation se produit lorsqu'un destinataire indique qu'il ne veut pas recevoir un e-mail. Ils ont peut-être cliqué sur le bouton « Signaler un spam » dans leur client de messagerie, se sont plaints auprès de leur fournisseur de messagerie, ont prévenu SES directement ou ont utilisé une autre méthode. Cette rubrique inclut des informations générales sur les réclamations. Si votre notification contient des informations spécifiques sur la source des plaintes, lisez également le sujet correspondant :

- FAQ sur les plaintes de SES via des boucles de feedback
- FAQ sur les plaintes de SES provenant directement des destinataires

- FAQ sur les plaintes de SES par le biais de fournisseurs de messagerie

Q2. En quoi ces réclamations vous gênent-elles ?

Les taux de réclamation élevés sont souvent utilisés par des entités telles que les fournisseurs de messagerie et les organisations anti-courrier indésirable pour déterminer si un expéditeur envoie des messages à des destinataires qui ne se sont pas spécifiquement inscrits pour recevoir des e-mails, ou si l'expéditeur envoie un contenu différent de celui auquel les destinataires se sont inscrits.

Q3. Que dois-je faire si je reçois un avis indiquant que mon compte est sous vérification ou que mes envois sont interrompus en raison d'un problème lié à des réclamations ?

Vérifiez votre processus d'acquisition de listes et le contenu de vos e-mails afin d'essayer de comprendre pourquoi vos destinataires peuvent ne pas apprécier les e-mails qu'ils reçoivent de votre part. Identifiez la cause du problème, puis corrigez-la. Après avoir apporté les modifications qui, selon vous, résoudront le problème, connectez-vous à la AWS console et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Dans le message, fournissez des informations détaillées sur les étapes que vous avez effectuées pour résoudre le problème et décrivez la manière dont ces étapes empêchent le problème de se reproduire.

Q4. Que puis-je faire pour limiter les réclamations ?

Tout d'abord, assurez-vous de suivre les plaintes que SES peut vous signaler, qui sont des plaintes que SES reçoit par le biais de boucles de rétroaction (voir leFAQ sur les plaintes de SES via des boucles de feedback). Ensuite, suivez ces instructions :

- N'achetez pas, ne louez pas ou ne partagez pas d'adresses e-mail. Utilisez uniquement les adresses qui ont demandé spécifiquement votre mail.
- Utilisez la double acceptation pour inscrire de nouveaux utilisateurs. En d'autres termes, lorsque de nouveaux utilisateurs s'inscrivent, envoyez-leur un e-mail de confirmation sur lequel ils doivent cliquer avant de recevoir tout e-mail supplémentaire. Ceci évite que certaines personnes en inscrivent d'autres, ainsi que les inscriptions accidentelles.
- Surveillez l'implication avec l'e-mail que vous envoyez et arrêtez l'envoi aux destinataires qui n'ont pas ouvert vos messages ou n'ont pas cliqué dessus.

- Lorsque de nouveaux utilisateurs s'inscrivent, indiquez clairement le type d'e-mail qu'ils recevront de votre part, et veillez à envoyer uniquement le type d'e-mail auquel ils se sont inscrits. Par exemple, si des utilisateurs s'inscrivent aux dernières actualités, ne leur envoyez pas de publicités.
- Assurez-vous que votre e-mail est bien formaté et a un aspect professionnel.
- Assurez-vous que votre e-mail est clairement de votre part et qu'il ne peut pas être confondu avec quelque chose d'autre.
- Fournissez aux utilisateurs un moyen simple et évident de se désabonner de votre e-mail.

FAQ sur les plaintes de SES via des boucles de feedback

Cette rubrique fournit des informations sur les plaintes que SES reçoit de la part de fournisseurs de messagerie par le biais de boucles de feedback. Pour obtenir des informations générales qui s'appliquent à tous les types de réclamations, consultez FAQ sur les réclamations.

Q1. Comment ce type de réclamation est-il signalé ?

La plupart des programmes clients de messagerie fournissent un bouton intitulé « Marquer comme courrier indésirable », ou similaire, qui permet de déplacer le message vers un dossier de courrier indésirable et de le transmettre au fournisseur de messagerie. De plus, la plupart des fournisseurs de messagerie gèrent une adresse « abuse » (par exemple, abuse@example.com), où les utilisateurs peuvent transférer les e-mails indésirables et demander au fournisseur de prendre des mesures préventives. Si SES a mis en place une boucle de feedback (FBL) avec le fournisseur de messagerie, celui-ci renvoie la plainte à SES.

> **Note**
>
> SES définit automatiquement l'en-tête Feedback-ID lorsque vous envoyez des messages, ce qui permet aux fournisseurs de boîtes aux lettres d'agréger les statistiques de livraison, telles que les taux de plaintes et de spam, et de les mettre à votre disposition. La valeur d'en-tête Feedback-ID fournie par SES est composée comme suit :
>
> - `FeedBackId:((SESInternalID):(AmazonSES))`, où :
>   - SESInternalID est l'identifiant utilisé par SES pour collecter les informations relatives aux plaintes.
>   - AmazonSES est une balise statique identifiant SES en tant que plateforme d'envoi.

En option, en plus de la valeur d'en-tête Feedback-ID standard fournie par SES, vous pouvez également spécifier vos propres identifiants de commentaires personnalisés (jusqu'à deux) à l'aide des balises de `ses:feedback-id-b` message `ses:feedback-id-a` et, voir. the section called “Feedback précis pour les campagnes par e-mail”

Q2. Ces plaintes sont-elles incluses dans les statistiques relatives au taux de plaintes affichées dans la console SES et renvoyées par l' GetSendStatistics API ?

Oui. Toutefois, les statistiques relatives au taux de plaintes n'incluent pas les plaintes émanant de fournisseurs de messagerie qui ne fournissent pas de commentaires à SES. Le taux de réclamation lié aux domaines qui fournissent des commentaires est susceptible d'être représentatif du reste de votre envoi également.

Q3. Comment puis-je être averti de ces réclamations ?

Vous pouvez recevoir une notification par e-mail ou par le biais de notifications Amazon SNS. Consultez les instructions de configuration dans Configuration de notifications d'événement pour Amazon SES.

Q4. Que dois-je faire si je reçois une notification de réclamation par e-mail ou par le biais d'Amazon SNS ?

Commencez par supprimer de votre liste de diffusion les adresses qui ont généré des réclamations et arrêtez immédiatement de les utiliser pour les envois. N'envoyez même pas d'e-mail indiquant que vous avez reçu la demande de désabonnement. Envisagez de configurer l'automatisation pour ce processus, soit en traitant par programme la boîte aux lettres dans laquelle vous recevez les réclamations, soit en configurant les notifications de réclamation à l'expéditeur via Amazon SNS. Pour plus d’informations, consultez Configuration de notifications d'événement pour Amazon SES.

Ensuite, examinez en détail votre envoi afin de déterminer pourquoi vos destinataires n'apprécient pas l'e-mail que vous envoyez et de résoudre ce problème sous-jacent. Pour chaque personne qui fait une réclamation, il y en a potentiellement plusieurs dizaines qui n'ont pas apprécié votre e-mail et qui n'ont pas fait (ou n'ont pas pu faire) de réclamation. Si vous vous contentez de supprimer les destinataires qui ont effectué une réclamation, vous ne réglez pas le problème sous-jacent.

Q5. Divulguez-vous les taux de plaintes de SES susceptibles d'entraîner la révision de mon compte ou de suspendre la capacité de mon compte à envoyer des e-mails ?

Pour un résultat optimal, vous devez maintenir un taux de réclamation inférieur à 0,1 %. Des taux de réclamation supérieurs peuvent avoir un impact sur la remise de vos e-mails.

Si votre taux de réclamation est de 0,1 % ou plus, nous placerons votre compte sous vérification. Si votre taux de réclamation est de 0,5 % ou plus, nous pouvons suspendre la capacité de votre compte à envoyer d'autres e-mails tant que vous n'avez pas résolu le problème à l'origine de ce taux élevé.

Q6. Pendant quelle période de temps mon taux de réclamation est-il calculé ?

Nous ne calculons pas votre taux de réclamation en fonction d'une durée fixée, car différents expéditeurs envoient à des taux différents. À la place, nous examinons un volume représentatif, c'est-à-dire une quantité d'e-mails qui représentent vos pratiques d'envoi habituelles. Afin d'être équitable à la fois pour les expéditeurs de volumes élevés et faibles, le volume représentatif est différent pour chaque utilisateur et évolue avec les tendances d'envoi de l'utilisateur. De plus, le taux de réclamation n'est pas calculé en fonction de chaque e-mail. Il est plutôt calculé comme le pourcentage de plaintes relatives aux e-mails envoyés aux domaines qui envoient des commentaires sur les plaintes à SES.

Q7. Puis-je calculer mon propre taux de plaintes en utilisant les métriques de la console SES ou de l'GetSendStatisticsAPI ?

Non. Ceci pour deux raisons principales :

- Le taux de réclamation est calculé à l'aide de volume représentatif (voir Q6. Pendant quelle période de temps mon taux de réclamation est-il calculé ?). En fonction de votre taux d'envoi, le taux de plaintes peut remonter bien au-delà de ce que la console ou l'`GetSendStatistics`API SES peut récupérer. C'est pourquoi nous vous recommandons d'utiliser régulièrement ces méthodes afin de surveiller le taux de réclamation pour votre compte. En surveillant ainsi votre taux de réclamation, vous obtenez les informations dont vous avez besoin pour détecter les problèmes avant qu'ils n'atteignent des niveaux susceptibles d'avoir un impact sur la remise de vos e-mails.
- Lors du calcul du taux de réclamation, tous les e-mails ne sont pas pris en compte. Le taux de plaintes est calculé comme le pourcentage de plaintes relatives aux e-mails envoyés aux domaines qui envoient des commentaires sur les plaintes à SES.

Q8. Comment puis-je connaître les adresses électroniques qui ont effectué une réclamation ?

Examinez les notifications de plainte que SES vous envoie par e-mail ou via Amazon SNS (voirConfiguration de notifications d'événement pour Amazon SES). Cependant, les différents fournisseurs de messagerie fournissent des quantités différentes d'informations, et certains expurgent l'adresse e-mail du destinataire avant de transmettre la notification de plainte à SES. Pour vous permettre de retrouver l'adresse e-mail du destinataire à l'avenir, la meilleure solution consiste à enregistrer votre propre mappage entre un identifiant et l'identifiant du message SES que SES vous transmet lorsqu'il accepte l'e-mail. Notez que SES ne conserve aucun identifiant de message personnalisé que vous ajoutez.

Q9. Si je n'ai pas surveillé mes réclamations, pouvez-vous me donner une liste d'adresses qui ont effectué une réclamation ?

Malheureusement, nous ne pouvons pas vous donner de liste exhaustive. Cependant, vous pouvez contrôler vos réclamations futures par e-mail ou via Amazon SNS.

Q10. Puis-je obtenir un exemple d'e-mail ?

Nous ne pouvons pas vous envoyer d'exemple d'e-mail sur demande, mais vous pouvez trouver ces informations dans la notification de réclamation. Pour plus d’informations, consultez Q8. Comment puis-je connaître les adresses électroniques qui ont effectué une réclamation ?.

FAQ sur les plaintes de SES provenant directement des destinataires

Cette rubrique fournit des informations sur les plaintes que SES reçoit directement des destinataires. Pour obtenir des informations générales qui s'appliquent à tous les types de réclamations, consultez FAQ sur les réclamations.

Q1. Comment ce type de réclamation est-il signalé ?

Plusieurs destinataires ont directement contacté SES à propos de votre courrier par e-mail ou par tout autre moyen.

Q2. Ces plaintes sont-elles incluses dans les statistiques relatives au taux de plaintes affichées dans la console SES et renvoyées par l' GetSendStatistics API ?

Non Les statistiques sur le taux de plaintes que vous récupérez à l'aide de la console SES ou de l'`GetSendStatistics`API incluent uniquement les plaintes que SES reçoit par le biais de boucles

de feedback. Pour en savoir plus sur ces types de réclamations, consultez FAQ sur les plaintes de SES via des boucles de feedback.

Q3. Pourquoi n'ai-je pas entendu parler de ces réclamations via des notifications de commentaires par e-mail ou via Amazon SNS ?

Le transfert de commentaires par e-mail et les notifications Amazon SNS incluent uniquement les plaintes que SES reçoit par le biais de boucles de feedback. Vous ne recevrez aucune notification concernant les plaintes déposées directement par les destinataires auprès de SES.

Q4. Comment puis-je connaître les adresses électroniques qui ont effectué une réclamation ?

Pour protéger les identités des destinataires ayant déposé des réclamations, nous ne pouvons pas répertorier les adresses e-mail ayant déposé des réclamations contre votre e-mail.

Plutôt que de vous concentrer sur la suppression de destinataires individuels de votre liste, nous vous recommandons de déterminer le problème ayant conduit au dépôt de réclamations. Nous vous recommandons de commencer par vérifier votre processus de prospection de clients, et de supprimer les clients de vos listes qui n'ont pas explicitement demandé à recevoir des e-mails de votre part. Vous devez également analyser le contenu de vos e-mails afin d'essayer de comprendre pourquoi vos destinataires se plaignent.

Q5. Puis-je obtenir un exemple d'e-mail ?

Pour protéger les identités des destinataires ayant déposé des réclamations, nous ne pouvons pas fournir de copies des e-mails ayant poussé vos destinataires à déposer des réclamations.

Q6. Que dois-je faire si je reçois une notification indiquant que mon compte est sous vérification ou que mes envois sont interrompus en raison de réclamations directes ?

Modifiez immédiatement votre processus d'envoi afin d'envoyer des messages uniquement aux destinataires spécifiquement inscrits pour les recevoir. De plus, assurez-vous que vous envoyez le type de contenu pour lequel vos destinataires se sont inscrits. Après avoir apporté les modifications qui, selon vous, résoudront le problème, connectez-vous à la AWS console et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Dans le message, fournissez des informations détaillées sur les étapes que vous avez effectuées pour résoudre le problème et décrivez la manière dont ces étapes empêchent le problème de se reproduire.

Si vous ne soumettez pas de demande de réexamen sous trois semaines et que nous recevons toujours des réclamations des destinataires directs, nous pouvons suspendre la capacité de votre compte à envoyer des e-mails.

FAQ sur les plaintes de SES par le biais de fournisseurs de messagerie

Cette rubrique fournit des informations sur les plaintes que SES reçoit par le biais de fournisseurs de messagerie (également appelés fournisseurs de boîtes aux lettres). Pour obtenir des informations générales qui s'appliquent à tous les types de réclamations, consultez FAQ sur les réclamations.

Q1. Comment ce type de réclamation est-il signalé ?

Un fournisseur de messagerie a signalé à SES qu'un nombre important de ses clients avaient marqué vos e-mails comme du spam. Le rapport a été fourni à SES par un moyen autre que les boucles de rétroaction décrites dans leFAQ sur les plaintes de SES via des boucles de feedback.

Q2. Ces plaintes sont-elles incluses dans les statistiques relatives au taux de plaintes affichées dans la console SES et renvoyées par l' GetSendStatistics API ?

Non Les statistiques sur le taux de plaintes que vous récupérez à l'aide de la console SES ou de l'`GetSendStatistics`API incluent uniquement les plaintes que SES reçoit par le biais de boucles de feedback.

Q3. Pourquoi n'ai-je pas entendu parler de ces réclamations via des notifications de commentaires par e-mail ou via Amazon SNS ?

Le transfert de commentaires par e-mail et les notifications Amazon SNS incluent uniquement les plaintes que SES reçoit par le biais de boucles de feedback.

Q4. Comment puis-je connaître les adresses électroniques qui ont effectué une réclamation ?

En règle générale, les fournisseurs d'e-mails ne divulguent pas ces informations. Cependant, au lieu de se concentrer sur la suppression des destinataires de votre liste, vous devez vous concentrer sur la recherche et la résolution du problème sous-jacent. Commencez par vérifier votre processus d'acquisition de listes et le contenu de vos e-mails afin d'essayer de comprendre pourquoi vos destinataires peuvent ne pas apprécier votre e-mail.

Q5. Puis-je obtenir un exemple d'e-mail ?

Non. En général, les fournisseurs de messagerie ne fournissent pas d'exemple d'e-mail.

Q6. Que dois-je faire si je reçois une notification indiquant que mon compte est sous vérification ou que mes envois sont interrompus en raison de réclamations de fournisseur de messagerie ?

Identifiez la cause du problème, puis corrigez-la. Après avoir apporté les modifications qui, selon vous, résoudront le problème, connectez-vous à la AWS console et accédez au Centre de

support. Répondez au cas que nous avons ouvert en votre nom. Dans le message, fournissez des informations détaillées sur les étapes que vous avez effectuées pour résoudre le problème et décrivez la manière dont ces étapes empêchent le problème de se reproduire. Si vous ne soumettez pas de demande de réexamen sous trois semaines et que nous recevons toujours des réclamations de fournisseurs, nous pouvons suspendre la capacité de votre compte à envoyer d'autres e-mails.

FAQ sur les pièges pour le courrier indésirable

Q1. Que sont les pièges pour le courrier indésirable ?

Un spamtrap (piège à spam) est une adresse e-mail spéciale gérée par un fournisseur d'accès Internet (FAI), un fournisseur de messagerie ou une organisation anti-courrier indésirable. Dans la mesure où cette adresse ne sera jamais légitimement inscrite pour recevoir les e-mails, les organisations qui gèrent ces pièges pour le courrier indésirable savent que toute personne qui envoie un e-mail à l'une de ces adresses se livre probablement à des pratiques de messagerie douteuses.

Q2. Comment les pièges pour le courrier indésirable sont-ils configurés ?

Les adresses des pièges pour le courrier indésirable peuvent être configurées de différentes manières. Elles peuvent être converties à partir d'adresses qui ont été valides, mais sont inutilisées (et reviennent à l'expéditeur) depuis longtemps. Ils peut également d'agir d'adresses qui ont été configurées uniquement pour être utilisées comme pièges pour le courrier indésirable. Ils peut s'agir d'adresses inhabituelles qui sont difficiles à deviner, et parfois d'adresses qui sont proches de véritables adresses (par exemple, avec une erreur ajoutée à un nom de domaine commun). Souvent, mais pas toujours, les pièges pour le courrier indésirable sont lancés dans le monde entier par le biais d'Internet de diverses manières.

Q3. Comment SES sait-il si j'envoie des messages vers des spamtraps ?

Certaines organisations qui exploitent des spamtraps envoient des notifications à SES lorsque leurs spamtraps sont touchés par des expéditeurs de SES.

Q4. Comment SES utilise-t-il les rapports anti-spam ?

Nous examinons les rapports. Si nous déterminons que votre compte envoie des e-mails vers des pièges pour le courrier indésirable, nous plaçons votre compte sous vérification et nous vous demandons de résoudre le problème sous-jacent. Si vous ne corrigez pas le problème avant la fin de la période de vérification, nous pouvons suspendre la capacité de votre compte à envoyer d'autres e-mails. Si votre de problème de piège pour le courrier indésirable est très grave, nous pouvons

suspendre immédiatement la capacité de votre compte à envoyer des e-mails, sans d'abord placer celui-ci sous vérification.

Q5. Que dois-je faire si je reçois un avis indiquant que mon compte est sous vérification ou que mes envois sont interrompus en raison d'un problème lié à des pièges pour le courrier indésirable ?

Tout d'abord, vous devez résoudre le problème qui nous a amenés à placer votre compte sous vérification ou à suspendre votre capacité d'envoi d'e-mails. Ensuite, connectez-vous à la AWS console et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Dans le message, fournissez des informations détaillées sur les étapes que vous avez effectuées pour résoudre le problème et décrivez la manière dont ces étapes empêchent le problème de se reproduire. Si nous jugeons que les modifications que vous avez effectuées traitent correctement le problème, nous annulerons la période de vérification ou nous mettrons fin à la suspension d'envoi à partir de votre compte.

En raison de la façon dont les e-mails piégés sont signalés, cela peut prendre trois semaines ou plus avant que nous puissions déterminer si les modifications que vous avez effectuées ont résolu le problème.

Q6. Combien d'envois d'e-mails vers des pièges pour le courrier indésirable puis-je effectuer avant que vous placiez mon compte sous vérification ou que vous suspendiez la capacité de mon compte à envoyer des e-mails ?

Nous ne divulguons pas le nombre spécifique d'e-mails piégés qui nous amènent à agir sur votre compte. Cependant, il est important de noter que même un petit nombre d'e-mails piégés peut avoir un impact très négatif sur votre réputation d'expéditeur. Vous devez donc prendre au sérieux les rapports sur les pièges pour le courrier indésirable.

Q7. Divulguez-vous les adresses des pièges pour le courrier indésirable ?

Non. Pour que les pièges pour les courriers indésirables soient efficaces, il est essentiel qu'ils restent confidentiels. Les organisations qui s'occupent des pièges pour le courrier indésirable divulguent uniquement le nombre d'adresses piégées, pas les adresses qui servent de piège.

Q8. Que puis-je faire pour éviter l'envoi vers des pièges pour le courrier indésirable ?

Pour réduire les risques d'envoi vers des pièges pour le courrier indésirable, suivez ces instructions :

- N'achetez pas, ne louez pas ou ne partagez pas d'adresses e-mail. Utilisez uniquement les adresses qui ont demandé spécifiquement votre mail.
- Sur les formulaires web, demandez aux utilisateurs d'entrer leurs adresses e-mail deux fois, et vérifiez que les deux adresses correspondent avant d'envoyer le formulaire.
- Utilisez la double acceptation pour inscrire de nouveaux utilisateurs. En d'autres termes, lorsque de nouveaux utilisateurs s'inscrivent, envoyez-leur un e-mail de confirmation sur lequel ils doivent cliquer avant de recevoir tout e-mail supplémentaire.
- Assurez-vous que vous supprimez de votre liste les adresses qui sont retournées à l'expéditeur définitivement, afin qu'elles soient supprimées bien avant d'être converties en pièges pour le courrier indésirable.
- Assurez-vous que vous surveillez l'implication de vos destinataires et arrêtez l'envoi aux destinataires qui n'ont pas consulté vos e-mails ou votre site web récemment. Les délais qui définissent un « utilisateur impliqué » dépendent de votre cas d'utilisation, mais en règle générale, si les utilisateurs n'ont pas ouvert ou cliqué sur vos e-mails depuis plusieurs mois, vous devez envisager de les supprimer à moins de disposer de preuves qu'ils souhaitent recevoir vos e-mails.
- Soyez très prudent avec les campagnes de réimplication dans le cadre desquelles vous contactez volontairement les personnes n'ayant pas interagi avec vous récemment. Ces efforts ont tendance à être hautement risqués et peuvent souvent entraîner des problèmes non seulement avec l'envoi vers des pièges pour le courrier indésirable, mais également avec les retours à l'expéditeur et les réclamations.
- Envoyez un message d'acceptation à l'ensemble de votre liste de diffusion et conservez uniquement les destinataires qui cliquent sur le lien de vérification. Outre la suppression de destinataires inactifs de votre liste, cette procédure contribue également à supprimer les adresses des pièges pour le courrier indésirable. Cependant, nous vous déconseillons d'utiliser cette technique si vous pensez que votre liste de diffusion peut contenir un grand nombre d'adresses non valides ou si votre compte a déjà un problème avec les retours à l'expéditeur, en raison des risques de voir le taux de retour de votre compte encore augmenter.

FAQ sur les enquêtes manuelles

Q1. Que dois-je faire si je reçois une notification indiquant que mon compte est sous vérification ou que mes envois sont interrompus en raison d'enquêtes manuelles ?

Un enquêteur de SES a identifié un problème important concernant votre envoi. Généralement, ces problèmes concernent les éléments suivants, mais sans s'y limiter :

- Votre envoi ne respecte pas la politique d'utilisation acceptable d'AWS (AUP).
- Vos e-mails semblent être non sollicités.
- Votre contenu est lié à l'hameçonnage (y compris l'hameçonnage simulé).
- Votre contenu est par ailleurs associé à un cas d'utilisation que SES ne prend pas en charge.

Si nous pensons que le problème peut être corrigé, nous plaçons votre compte sous vérification pendant un certain laps de temps. Pendant que votre compte est sous vérification, vous devez apporter des modifications à vos pratiques d'envoi d'e-mails pour corriger le problème.

Si nous ne pensons pas que le problème peut être corrigé, ou si le problème est très grave, nous pouvons suspendre la capacité de votre compte à envoyer des e-mails sans d'abord placer celui-ci sous vérification.

Q2. Quels problèmes peuvent vous amener à effectuer une vérification manuelle de mes envois d'e-mails ?

Plusieurs problèmes peuvent nous amener à commencer une vérification manuelle de votre compte. Il s'agit notamment des raisons suivantes, sans s'y limiter :

- Les destinataires contactent SES pour se plaindre des e-mails envoyés depuis votre compte.
- Nous détectons des changements inhabituels dans vos schémas d'envoi d'e-mails.
- Nos filtres anti-spam détectent des caractéristiques de vos e-mails qui sont typiques des contenus indésirables ou de mauvaise qualité.

Nous vous envoyons une notification lorsque nous plaçons votre compte sous vérification ou suspendons sa capacité à envoyer des e-mails. Dans la plupart des cas, cette notification contient des détails sur le problème et fournit des informations sur les étapes suivantes que vous pouvez effectuer.

Q3. Qu'est-ce qu'un e-mail « non sollicités » ?

Les e-mails non sollicités sont des e-mails que le destinataire n'a pas explicitement demandé à recevoir. Cela inclut les cas où un destinataire s'inscrit à un certain type d'e-mail (par exemple, des notifications) et reçoit à la place un différent type d'e-mail (par exemple, des publicités).

Nous vous envoyons une notification lorsque nous plaçons votre compte sous vérification ou suspendons sa capacité à envoyer des e-mails. Si vous recevez une notification indiquant que nous

prenons l'une de ces mesures en raison d'un problème lié à un e-mail non sollicité, connectez-vous à la AWS console et rendez-vous au Centre de Support. Répondez au cas que nous avons ouvert en votre nom. Dans votre message, incluez les informations suivantes :

- Tous les messages que vous envoyez ont-ils été spécifiquement demandés par le destinataire et respectent-ils la politique d'utilisation acceptable d'AWS ?
- Avez-vous acquis des adresses e-mail autrement que par le biais d'une interaction spécifique du client avec vous ou votre site web et d'une demande d'e-mails à partir de celui-ci ? Vous devez expliquer comment vous avez fait l'acquisition de votre liste de diffusion.
- Comment fonctionnent vos processus d'inscription et d'annulation d'inscription ? Vous devez inclure des liens d'acceptation et de refus.

Q4. Que dois-je faire si je reçois une notification indiquant que mon compte est sous vérification ou que mes envois sont interrompus en raison d'une vérification manuelle ?

Identifiez la cause du problème, puis corrigez-la. Après avoir apporté les modifications qui, selon vous, résoudront le problème, connectez-vous à la AWS console et accédez au Centre de support. Répondez au cas que nous avons ouvert en votre nom. Dans le message, fournissez des informations détaillées sur les étapes que vous avez effectuées pour résoudre le problème et décrivez la manière dont ces étapes empêchent le problème de se reproduire. Si nous jugeons que les modifications que vous avez effectuées traitent correctement le problème, nous annulerons la période de vérification de votre compte.

Q5. Quels types de problèmes considérez-vous comme « corrigeables » ?

En général, nous pensons que la situation peut être corrigée si vous avez un historique des bonnes pratiques en matière d'envoi et si vous pouvez prendre des mesures pour éliminer les envois problématiques, tout en continuant la plus grande partie de votre envoi. Par exemple, si vous envoyez trois types d'e-mails différents et qu'un seul type pose un problème, vous pouvez simplement arrêter l'envoi problématique et continuer avec le reste de votre envoi.

Q6. Que faire si je ne parviens pas à trouver l'origine du problème ?

Vous pouvez vous connecter à la AWS console et accéder au Centre de support. Répondez au cas que nous avons ouvert en votre nom et demandez un exemple d'e-mail à l'origine du problème.

FAQ sur les listes DNSBL (DNS Blackhole Lists)

Les listes DNSBL (Domaine Name System-based Blackhole Lists), parfois appelées listes RBL (Realtime Blackhole Lists), listes de refus, listes de blocage ou listes d'exclusion, servent à indiquer aux fournisseurs de messagerie les adresses IP soupçonnées d'envoyer des e-mails indésirables.

Différentes listes DNSBL ont des impacts distincts sur la délivrabilité des e-mails. Cette rubrique décrit comment les listes DNSBL peuvent avoir un impact sur la remise des e-mails que vous envoyez avec Amazon SES, ainsi que nos stratégies de suppression des adresses IP Amazon SES des listes DNSBL.

> **Note**
>
> Cette rubrique concerne les listes DNSBL qu'utilisent les fournisseurs de messagerie pour bloquer les messages entrants. Pour de plus amples informations sur la façon dont Amazon SES bloque les messages sortants envoyés à des destinataires dont les adresses ont déjà occasionné des retours à l'expéditeur, veuillez consulter Liste de suppression globale Amazon SES.

Q1. Comment les listes DNSBL impactent-elles la remise d'e-mails ?

Différentes listes DNSBL ont des impacts distincts sur la réussite de la remise d'un message. Les principaux fournisseurs de messagerie, y compris Gmail, Hotmail, AOL, et Yahoo, semblent reconnaître un très petit nombre de listes DNSBL très respectées, telles que celles proposées par Spamhaus. D'après notre expérience, d'autres listes DNSBL ont tendance à avoir un faible impact, même si des systèmes de messagerie privilégient certaines listes DNSBL par rapport à d'autres.

Enfin, de nombreux fournisseurs de messagerie possèdent leurs propres listes de refus internes. Les fournisseurs de messagerie protègent généralement ces listes très étroitement et les partagent rarement avec le public. Si une adresse IP se trouve sur l'une de ces listes, elle peut avoir un impact majeur sur votre capacité à envoyer des e-mails à des destinataires qui utilisent ce fournisseur.

Q2. Comment les adresses IP se retrouvent-elles sur des listes DNSBL ?

Il existe plusieurs façons pour une adresse IP de se retrouver sur une liste DNSBL. Les adresses IP peuvent être ajoutées aux listes DNSBL lorsqu'elles envoient un e-mail à un piège pour le courrier indésirable. Un piège pour le courrier indésirable est une adresse e-mail qui n'appartient pas à un

utilisateur humain. Ces pièges existent uniquement pour recueillir le courrier indésirable et identifier leurs expéditeurs. Certaines listes DNSBL autorisent aussi les utilisateurs individuels à envoyer des adresses IP. Quelques listes DNSBL permettent aux utilisateurs de soumettre des plages complètes d'adresses IP. D'autres listes DNSBL sont gérées via les contributions des administrateurs de messagerie et peuvent inclure des adresses IP quand les administrateurs pensent que celles-ci abusent de leurs propres systèmes.

Q3. Comment Amazon SES empêche les adresses IP d'apparaître sur les listes DNSBL ?

Nos systèmes recherchent les signes d'abus. Si nous détectons des modèles d'envoi ou d'autres caractéristiques pouvant entraîner la mise sur liste DNSBL d'une adresse IP, nous envoyons une notification à l'expéditeur. Si la situation est grave, ou si l'expéditeur ne résout pas le problème après que nous avons envoyé la notification, nous suspendons la capacité de l'expéditeur à envoyer des e-mails tant qu'il n'a pas résolu ce problème. En appliquant ainsi nos stratégies d'envoi, nous contribuons à réduire les risques que nos adresses IP se retrouvent sur des listes DNSBL.

Q4. Est-il possible pour Amazon SES que ses adresses IP soient supprimées d'une liste DNSBL ?

Nous surveillons activement les listes DNSBL qui pourraient avoir un impact sur la livraison de l'ensemble du service Amazon SES, ou un impact sur la capacité à envoyer des e-mails aux destinataires qui utilisent des fournisseurs de messagerie majeurs, comme Gmail, Yahoo, AOL et Hotmail. Les listes DNSBL proposées par Spamhaus entrent dans cette catégorie. Lorsque l'une de nos adresses IP apparaît sur une liste qui répond à l'un ou l'autre de ces critères, nous prenons des mesures immédiates pour que cette adresse soit supprimée de la liste DNSBL aussi rapidement que possible.

Nous ne surveillons pas les listes DNSBL qui sont susceptibles d'influer sur la livraison dans l'ensemble du service Amazon SES, ou qui n'ont pas un impact mesurable sur la livraison aux fournisseurs de messagerie majeurs. Les listes DNSBL proposées par SORBS et UCEPROTECT entrent dans cette catégorie. En raison des pratiques spécifiques de mise en vente et de radiation des listes des fournisseurs qui exploitent ces listes, nous ne sommes pas en mesure de supprimer nos adresses IP de ces listes.

Q5. Un fournisseur d'e-mails rejette mes e-mails, car l'adresse IP d'envoi est répertoriée par une liste DNSBL autre que Spamhaus. Que puis-je faire ?

Tout d'abord, vérifiez que le message a été vraiment bloqué en raison de sa présence sur une liste DNSBL. Si votre e-mail a été rejeté parce que l'adresse IP d'envoi était en liste DNSBL, vous recevrez une notification de retour à l'expéditeur indiquant le nom du fournisseur de liste DNSBL, comme dans l'exemple suivant :

```
554 5.7.1 Service unavailable; Client host [192.0.2.0] blocked using DNSBLName;
 See: http://www.example.com/query/ip/192.0.2.0
```

Si vous avez reçu une notification de retour à l'expéditeur, mais qu'elle ne contenait pas d'informations similaires au message de l'exemple précédent, le fournisseur de messagerie a très probablement rejeté votre message pour une raison non liée à une liste DNSBL.

Si vous pouvez confirmer qu'un fournisseur de messagerie bloque vos e-mails parce que l'adresse IP d'envoi figure sur une liste DNSBL, voici quelques mesures que vous pouvez prendre :

- Contacter l'administrateur du domaine qui a rejeté votre message pour demander une exception à sa stratégie de filtrage du courrier indésirable. Certains administrateurs ont des processus de support et peuvent publier une page d'administrateur qui décrit ce processus. Si le domaine que vous essayez de contacter ne publie pas ses stratégies de support administrateur, vous pouvez peut-être contacter l'administrateur en envoyant un e-mail à postmaster@*exemple.com*, où *exemple.com* est le domaine en question. Les domaines sont tenus en vertu de la spécification RFC 5321 de disposer d'une boîte aux lettres d'administrateur.

  Lorsque vous contactez l'administrateur, fournissez les codes de retour à l'expéditeur que vous avez reçus, les en-têtes de l'e-mail que vous essayez d'envoyer, une évaluation de l'impact que la liste DNSBL a sur la remise de vos e-mails, et la raison pour laquelle vous pensez que votre e-mail est bloqué à tort. Plus vous pourrez fournir des informations à l'administrateur pour démontrer que vous envoyez des e-mails légitimes, plus l'administrateur sera susceptible de faire une exception pour vous.
- Si le fournisseur de messagerie ne répond pas ou ne veut pas modifier ses stratégies, envisagez d'utiliser une adresse IP dédiée. Les adresses IP dédiées sont des adresses que vous seul(e) pouvez utiliser. En implémentant les bonnes pratiques d'envoi, vous pouvez conserver un taux d'engagement élevé, et des taux très bas de retours à l'expéditeur, de réclamations et de pièges

pour le courrier indésirable. Des pratiques d'envoi appropriées peuvent vous aider à vous assurer que vos adresses ne finissent pas sur des listes DNSBL.

Q6. Un e-mail que j'envoie à Gmail, Yahoo, Hotmail ou un autre fournisseur majeur, est envoyé au dossier de courrier indésirable. Cela se produit-il parce que mon adresse IP d'envoi est inscrite sur une liste DNSBL ?

Probablement pas. Si une adresse IP est répertoriée par une liste DNSBL ayant un impact significatif, telle que l'une des listes DNSBL de Spamhaus, les principaux fournisseurs de messagerie rejettent complètement l'e-mail de cette adresse IP, plutôt que de l'envoyer dans le dossier courrier indésirable.

Lorsque les fournisseurs de messagerie majeurs acceptent un e-mail (au lieu de le rejeter), ils tiennent généralement compte de l'implication des utilisateurs pour déterminer s'il faut les placer dans la boîte de réception ou dans le dossier de courrier indésirable. L'engagement utilisateur fait référence aux façons dont les utilisateurs ont interagi avec les messages que vous leur avez envoyés précédemment.

Pour augmenter les chances que vos messages atteignent les boîtes de réception de vos clients, vous devez mettre en œuvre toutes les bonnes pratiques suivantes :

- Ne jamais louer ou acheter des listes d'adresses électroniques. La location ou l'achat de listes est une violation de la stratégie d'utilisation acceptable AWS (AUP) et n'est autorisée en aucun cas sur Amazon SES.
- Envoyer les e-mails uniquement aux clients qui ont explicitement demandé à en recevoir de votre part. Dans de nombreux pays et juridictions à travers le monde, il est illégal d'envoyer des e-mails à des destinataires qui n'ont pas explicitement accepté de les recevoir de votre part.
- Arrêter l'envoi d'e-mails aux clients qui n'ont pas ouvert ou cliqué sur les liens des messages que vous avez envoyés au cours des 30 à 90 derniers jours. Cette étape peut vous aider à maintenir vos taux d'engagement élevés, ce qui augmente les chances que les messages envoyés à l'avenir arrivent dans les boîtes de réception des destinataires.
- Utiliser des éléments de conception et des styles d'écriture cohérents d'un message à l'autre afin de garantir que les clients puissent facilement identifier vos messages.
- Utiliser des mécanismes d'authentification d'e-mail comme SPF et DKIM.
- Lorsque les clients utilisent un formulaire web pour s'abonner à votre contenu, envoyez-leur un e-mail pour confirmer qu'ils veulent recevoir vos e-mails. Ne pas envoyer d'autres e-mails tant que

les clients n'ont pas confirmé qu'ils souhaitaient recevoir vos e-mails. Ce processus est connu sous le nom d'acceptation confirmée ou de confirmation d'acceptation.

- Faire en sorte que les clients puissent se désabonner facilement et respecter immédiatement les demandes de désabonnement.
- Si vous envoyez un e-mail contenant des liens, vérifiez ces liens par rapport à la liste DBL (Domain Block List) de Spamhaus. Pour tester vos liens, utilisez l'outil de recherche de domaine sur le site web de Spamhaus.

En implémentant ces pratiques, vous pouvez améliorer votre réputation d'expéditeur, ce qui augmente la probabilité que les e-mails que vous envoyez arrivent dans les boîtes de réception des destinataires. La mise en œuvre de ces pratiques peut également vous aider à conserver un taux bas de retours à l'expéditeur et de réclamations pour votre compte, et à réduire le risque d'envoi d'e-mails vers des pièges pour le courrier indésirable.

FAQ sur les métriques Amazon SES d'envoi d'e-mails

Amazon SES prélève plusieurs métriques sur les e-mails que vous envoyez. Ces métriques vous permettent d'analyser l'efficacité de votre programme de messagerie électronique et de surveiller des statistiques importantes, telles que les taux de retours à l'expéditeur et de réclamations.

Cette section contient les questions fréquentes sur les rubriques suivantes liées aux métriques d'envoi d'e-mails :

- Questions d'ordre général
- Suivi des ouvertures
- Suivi des clics

> **Note**
>
> Le suivi des événements repose sur le fournisseur de services de messagerie (ESP) du destinataire et la configuration de ses paramètres de confidentialité. Cela échappe au contrôle d'Amazon SES. Le nombre d'événements de suivi peut être biaisé (renvoi des nombres incorrects) dans les situations suivantes :
>
> - Le destinataire de l'e-mail utilise un fournisseur de services de messagerie (ESP) qui protège sa confidentialité.

- Le destinataire de l'e-mail n'autorise explicitement pas son fournisseur de services de messagerie (ESP) à partager ses données.
- Le fournisseur de services de messagerie (ESP) du destinataire de l'e-mail met en cache les images ou les liens. SES peut comptabiliser l'ouverture initiale, mais ne sera pas à même de compter les ouvertures suivantes.

Questions d'ordre général

Q1. Après la remise d'un e-mail, pendant combien de temps Amazon SES continue-t-il à collecter les métriques d'ouverture et de clic ?

Amazon SES collecte les métriques d'ouverture et de clic pendant 60 jours après chaque envoi d'e-mail.

Q2. Si un utilisateur ouvre un e-mail plusieurs fois ou clique sur un lien dans un e-mail plusieurs fois, chacun de ces événements est-il suivi séparément ?

Si un destinataire ouvre un e-mail plusieurs fois, Amazon SES compte chaque ouverture comme un événement d'ouverture unique. De même, si un destinataire clique sur le même lien plusieurs fois, Amazon SES compte chaque clic comme un événement de clic unique. Ces décomptes peuvent toutefois être faussés par les scénarios décrits ci-dessus dans la zone de notes.

Q3. Les métriques d'ouverture et de clic sont-elles regroupées ou peuvent-elles être mesurées au niveau des destinataires ?

Les ouvertures et les clics sont suivis au niveau du destinataire. Avec le suivi des ouvertures et des clics, vous pouvez déterminer quels destinataires ont ouvert un e-mail ou cliqué sur un lien dans un e-mail.

Q4. Puis-je récupérer les métriques d'ouverture et de clic à l'aide de l'API Amazon SES ?

L'API Amazon SES ne fournit pas de méthode pour la récupération des métriques d'ouverture et de clic. Cependant, vous pouvez récupérer les métriques d'ouverture et de clic pour Amazon SES à l'aide de l'API CloudWatch. Par exemple, vous pouvez utiliser l'AWS CLI pour récupérer les métriques de clic à l'aide de l'API CloudWatch en exécutant la commande suivante :

```
aws cloudwatch get-metric-statistics --namespace AWS/SES --metric-name Click \
  --statistics Sum --period 86400 --start-time 2017-01-01T00:00:00Z \
  --end-time 2017-12-31T23:59:59Z
```

La commande affichée ci-dessus récupère le nombre total d'événements de clic pour chaque journée de 2017. Pour récupérer les métriques d'ouverture, modifiez la valeur du paramètre `metric-name` en `Open`. Vous pouvez également modifier les paramètres `start-time` et `end-time` pour changer la période d'analyse, ou modifier le paramètre `period` pour une analyse plus détaillée.

Suivi des ouvertures

Q1. Comment fonctionne le suivi des ouvertures ?

Une image GIF transparente de 1 pixel par 1 pixel est insérée dans chaque e-mail envoyé via Amazon SES et inclut une référence unique à ce fichier d'image ; lorsque l'image est téléchargée, Amazon SES peut savoir exactement quel message a été ouvert et par qui.

Par défaut, ce pixel est inséré en bas de l'e-mail. Toutefois, les applications de certains fournisseurs de messagerie tronquent l'aperçu d'un e-mail lorsqu'il dépasse une certaine taille et peuvent fournir un lien pour afficher le reste du message. Dans ce scénario, l'image de suivi des pixels SES ne se charge pas et supprimera les taux d'ouverture que vous tentez de suivre. Pour contourner ce problème, vous pouvez éventuellement placer le pixel au début de l'e-mail, ou n'importe où ailleurs, en insérant l'espace réservé `{{ses:openTracker}}` dans le corps de l'e-mail. Une fois que SES aura reçu le message avec l'espace réservé, il sera remplacé par une image de pixel de suivi ouverte.

> **Important**
>
> Ajoutez un seul espace réservé `{{ses:openTracker}}`, car au-delà, un code d'erreur `400 BadRequestException` est renvoyé.

L'ajout du pixel de suivi ne modifie pas l'aspect de votre e-mail.

Q2. Le suivi des ouvertures est-il activé par défaut ?

Le suivi des ouvertures est disponible pour tous les utilisateurs Amazon SES par défaut. Pour utiliser le suivi des ouvertures, vous devez effectuer les opérations suivantes :

1. Crée un jeu de configurations.
2. Dans le jeu de configurations, créez une destination d'événement.
3. Configurez la destination d'événement pour publier des notifications d'événement d'ouverture sur une destination.
4. Dans chaque e-mail pour lequel vous souhaitez suivre les ouvertures, spécifiez le jeu de configurations que vous avez créé à l'étape 1.

Pour plus d'informations sur la façon d'activer le suivi ouvert via la destination des événements d'un jeu de configurations, voir the section called “Créer des destination d'évenement”. Vous pouvez utiliser l'espace réservé aux pixels dans Messagerie SMTPdans un e-mail formaté, brut et modélisé.

Découvrez comment Surveillance de l'envoi d'e-mails à l'aide de la publication d'événements.

Q3. Puis-je omettre le pixel de suivi d'ouverture dans certains e-mails ?

Il existe deux manières d'omettre le pixel de suivi d'ouverture dans vos e-mails. La première méthode consiste à envoyer l'e-mail sans spécifier un jeu de configurations. Vous pouvez également spécifier un jeu de configurations qui n'est pas configuré pour publier des données sur les événements d'ouverture.

Q4. Suivez-vous les ouvertures pour les e-mails en texte brut ?

Le suivi des ouvertures ne fonctionne qu'avec les e-mails HTML. Dans la mesure où le suivi des ouvertures s'appuie sur l'inclusion d'une image, il n'est pas possible de collecter les métriques d'ouverture pour les utilisateurs qui n'ouvrent les e-mails qu'à l'aide d'un client de messagerie texte uniquement (non HTML).

Suivi des clics

Q1. Comment fonctionne le suivi des clics ?

Pour suivre les clics, Amazon SES modifie chaque lien dans le corps de l'e-mail. Lorsque les destinataires ouvrent un lien, ils sont renvoyés vers un serveur Amazon SES et immédiatement acheminés vers l'adresse de destination. Comme pour le suivi des ouvertures, chaque lien de redirection est unique. Ceci permet à Amazon SES de déterminer quel destinataire a cliqué sur le lien, quand il a cliqué dessus et l'e-mail à partir duquel il est arrivé au lien.

> **Important**
>
> Si vous envoyez un seul message à plusieurs destinataires, chaque destinataire enregistre le même lien de suivi de clic. Pour suivre l'activité de clic de vos destinataires individuels, envoyez un e-mail à un seul destinataire par opération d'envoi.

Q2. Puis-je désactiver le suivi des clics ?

Vous pouvez désactiver le suivi des clics pour des liens individuels en ajoutant un attribut, `ses:no-track`, aux balises d'ancrage du corps HTML de votre e-mail. Par exemple, si vous créez un lien vers la page d'accueil AWS, un lien d'ancrage normal ressemble à ce qui suit :

```
<a href="https://aws.amazon.com">Amazon Web Services</a>
```

Pour désactiver le suivi des clics pour ce lien, modifiez-le de sorte qu'il ressemble à ce qui suit :

```
<a ses:no-track href="aws.amazon.com">Amazon Web Services</a>
```

Dans la mesure où `ses:no-track` n'est pas un attribut HTML standard, Amazon SES le supprime automatiquement de la version de l'e-mail qui arrive dans les boîtes de réception de vos destinataires.

Vous pouvez également désactiver le suivi des clics pour tous les messages que vous envoyez à l'aide d'un jeu de configurations spécifique. Pour désactiver le suivi des clics, modifiez la destination de l'événement du jeu de configurations afin qu'il ne capture pas les événements de clic.

Pour plus d'informations sur la façon d'activer et de désactiver le suivi des clics via la destination des événements d'un jeu de configurations, voir the section called “Créer des destination d'évenement”.

Découvrez comment Surveillance de l'envoi d'e-mails à l'aide de la publication d'événements.

Q3. Combien de liens peut-on suivre dans chaque e-mail ?

Le système de suivi des clics peut suivre 250 liens au maximum.

Q4. Les métriques de clic sont-elles recueillies pour les liens des e-mails en texte brut ?

Le suivi des clics est possible uniquement dans les e-mails au format HTML.

Q5. Puis-je baliser les liens avec des identificateurs uniques ?

Vous pouvez ajouter un nombre illimité de balises, sous la forme de paires clé-valeur, aux liens de votre e-mail à l'aide de l'attribut `ses:tags`. Lorsque vous utilisez cet attribut, spécifiez les clés et les valeurs en utilisant le même format que celui que vous utiliseriez pour transmettre les propriétés CSS en ligne : tapez la clé suivie de deux-points (:) et de la valeur. Si vous avez besoin de transmettre plusieurs paires clé-valeur, séparez chaque paire par un point-virgule (;).

Par exemple, supposons que vous vouliez ajouter les balises `product:book, genre:fiction, subgenre:scifi, type:newrelease` à un lien. Le lien obtenu ressemble à ce qui suit :

```
<a ses:tags="product:book;genre:fiction;subgenre:scifi;type:newrelease;"
    href="http://www.amazon.com/…/">New Releases in Science Fiction</a>
```

Ces balises sont transmises à la destination de publication de votre événement afin que vous puissiez effectuer une analyse supplémentaire sur les liens spécifiques sur lesquels vos utilisateurs ont cliqué.

> **Note**
>
> Les balises de lien peuvent inclure les chiffres de 0 à 9, les lettres A - Z (majuscules et minuscules), des tirets (-) et des traits de soulignement (_).

Q6. Les liens suivis utilisent-ils le protocole HTTP ou HTTPS ?

Les liens de suivi utilisent le même protocole que les liens originaux de votre e-mail.

Par exemple, si votre e-mail inclut un lien vers `https://www.amazon.com`, le lien est remplacé par un lien de suivi qui utilise le protocole HTTPS. Si votre e-mail inclut un lien vers `http://www.example.com`, le lien est remplacé par un lien de suivi qui utilise le protocole HTTP. Si votre e-mail inclut à la fois les liens mentionné précédemment, le lien HTTPS est remplacé par un lien de suivi qui utilise le protocole HTTPS et le lien HTTP est remplacé par un lien de suivi qui utilise le protocole HTTP.

Q7. Un lien dans mes e-mails n'est pas suivi. Pourquoi ?

Amazon SES s'attend à ce que les liens figurant dans vos e-mails contiennent des URL encodées correctement. Les URL de vos liens doivent plus particulièrement être conformes à RFC 3986. Si

un lien dans un e-mail n'est pas codé correctement, les destinataires le verront tout de même, mais Amazon SES ne suivra pas les événements de clic associés à ce lien.

Les problèmes liés à un encodage incorrect se produisent généralement dans les URL qui contiennent des chaînes de requête. Par exemple, si l'URL d'un lien dans votre e-mail contient un caractère espace non codé dans la chaîne de requête (par exemple, l'espace entre « John » et « Doe » dans l'exemple suivant : http://www.example.com/path/to/page?name=John Doe), Amazon SES ne suivra pas ce lien. Toutefois, si l'URL utilise un caractère espace non codé à la place (par exemple, « %20 » dans l'exemple suivant : http://www.example.com/path/to/page?name=John%20Doe), Amazon SES la suit comme prévu.

Index de recherche rapide

L'index suivant a été créé pour vous aider à trouver rapidement des éléments dans Amazon SES en proposant deux méthodes de recherche : par procédures ou par concepts. Les procédures décrivent « comment » effectuer une tâche tandis que les concepts expliquent la situation dans son ensemble.

Dites-nous ce que vous en pensez

Veuillez utiliser le bouton Feedback (Commentaires) dans le coin supérieur droit pour nous faire part de vos commentaires…

- Cet index vous a-t-il été utile ?
- Y a-t-il des procédures ou des concepts que vous aimeriez voir ajoutés à cet index ?
- Y a-t-il quelque chose qui, selon vous, aurait dû être catégorisé différemment ?

Liens vers les procédures et les concepts SES

How-tos

Les liens vers le mode d'emploi SES sont classés par ordre alphabétique et vous redirige vers la section correspondante pour vous montrer « comment » effectuer l'action que vous avez sélectionnée.

- Découvrez comment…
  - Ajouter un enregistrement SPF dans le cadre de la configuration d'un domaine MAIL FROM personnalisé
  - Attribuer des groupes d'adresses
  - Bloquer le SPAM pour la réception d'e-mails
  - Configurer les domaines personnalisés d'ouverture/de clic
  - Configurer les notifications SNS
  - Connexion à un point de terminaison SMTP
  - Créer un jeu de configurations
  - Créer une identité de domaine
  - Créer une identité d'adresse e-mail

- Créer des destination d'évenement
- Créer des filtres d'adresses IP
- Création d'un groupe d'adresses IP gérées pour activer des adresses IP dédiées (gérées)
- Créer des règles de réception
- Créer des alarmes de réputation à l'aide de CloudWatch
- Créer une politique d'autorisation d'envoi à l'aide d'une politique personnalisée
- Créer une politique d'autorisation d'envoi à l'aide du générateur de politiques
- Création de groupes d'adresses IP dédiées standard pour des adresses IP dédiées (standard)
- Supprimer une identité
- Supprimer les données personnelles
- Modifier une identité
- Activer le transfert de commentaires par e-mail
- Exporter les métriques de réputation
- Sortir de l'environnement de test (sandbox)
- Commencer avec SES
- Démarrer avec Virtual Deliverability Manager
- Accorder des autorisations pour la réception d'e-mails
- Augmenter le débit
- Augmenter votre quota d'envoi
- Intégration à votre serveur d'e-mail existant
- Journaliser les appels d'API
- Gérer un jeu de configuration
- Gérer Easy DKIM et BYODKIM
- Surveiller les métriques d'envoi et de réputation
- Surveiller les statistiques d'envoi
- Surveiller les statistiques d'utilisation
- Surveiller votre quota d'envoi
- Obtenir des enregistrements DKIM pour une identité
- Obtenir des informations d'identification SMTP

- Remplacer la suppression au niveau du compte par une suppression au niveau du jeu de configuration
- Remplacer la signature DKIM héritée sur une identité d'adresse e-mail
- Suspendre l'envoi d'e-mails
- Publier un enregistrement MX
- Signaler une utilisation abusive de ressources AWS
- Demander des adresses IP dédiées
- Demander une assistance technique
- Résoudre des problèmes de délivrabilité et de réputation à l'aide du conseiller Virtual Deliverability Manager
- Récupérer des données d'événements à partir de CloudWatch
- Récupérer des données d'événements à partir de Kinesis Data Firehose
- Récupérer des données d'événements à partir de SNS
- Envoyer un e-mail à l'aide d'un kit SDK AWS
- Envoyer des e-mails par programmation
- Envoyer un e-mail à l'aide de l'API SES
- Envoyer un e-mail à l'aide de SMTP
- Envoyer un e-mail brut avec une pièce jointe à l'aide de l'interface de ligne de commande ou de l'API SES
- Envoyer des e-mails de test à l'aide du simulateur de boîte aux lettres
- Configurer BYODKIM (Bring Your Own DKIM) (Apportez votre propre DKIM)
- Configurer une politique DMARC
- Configurer Easy DKIM
- Configurer la réception d'e-mails
- Configurer la publication d'événements
- Configurer un domaine MAIL FROM
- Configurer l'autorisation d'envoi (tâches de propriétaire d'identité)
- Configurer l'autorisation d'envoi (tâches d'expéditeur délégué)
- Spécifier un jeu de configuration lors de l'envoi d'e-mail
- Tester votre connexion à l'interface SMTP
- Suivre les taux de retour à l'expéditeur et de réclamation

- Comprendre les propriétés de signature DKIM héritées
- Utiliser les métriques de réputation
- Utiliser des packages logiciels pour envoyer des e-mails
- Utiliser la gestion des abonnements
- Utiliser des modèles pour envoyer des e-mails
- Utiliser votre liste de suppression au niveau du compte
- Vérifier l'identité d'un domaine
- Vérifier l'identité d'une adresse e-mail
- Afficher une identité
- Consultez l'ensemble et les détails des indicateurs de délivrabilité de votre compte à l'aide du tableau de bord Virtual Deliverability Manager
- Afficher les métriques SNDS pour les adresses IP dédiées
- Préparer les adresses IP dédiées

Concepts

Les liens vers les concepts SES sont classés par ordre alphabétique et vous dirigent vers le chapitre et les sections correspondants pour expliquer le concept que vous avez sélectionné.

- Trouver des informations sur…
  - Utilisation abusive de ressources AWS, signaler
  - Tableau de bord du compte
  - Liste de suppression au niveau du compte
  - Options d'action pour la réception d'e-mails
  - Action d'ajout d'en-tête
  - Types de pièces jointes, non prises en charge
  - Action de réponse de retour à l'expéditeur, retour
  - BYODKIM (Bring Your Own DKIM) (Apportez votre propre DKIM)
  - BYOIP (Bring Your Own IP) (Apportez votre propre IP)
  - Exemples de code
  - Validation de la conformité
  - Suppression au niveau du jeu de configuration

- Jeux de configurations
- Encodage de contenu
- Prise en charge de l'héritage des notifications entre comptes
- Domaine MAIL FROM personnalisé
- Protection des données
- Adresses IP dédiées
- Adresses IP dédiées (gérées)
- Adresses IP dédiées (standard)
- DKIM, authentification d'e-mail avec
- DMARC (Domain-based Message Authentication, Reporting and Conformance) (Authentification, rapport et conformité des messages basés sur le domaine)
- DMARC via DKIM, conformité à
- DMARC via SPF, conformité à
- Easy DKIM
- Destination du transfert de commentaires par e-mail
- Authentification de réception d'e-mail
- Concepts liés à la réception d'e-mails
- Instructions pour la console de réception d'e-mails
- Recherche de logiciels malveillants liés à la réception d'e-mails
- Autorisations liées à la réception d'e-mails
- Cas d'utilisation liés à la réception d'e-mails
- Restrictions liées à la réception d'e-mails
- Méthodes d'authentification liées à l'envoi d'e-mails
- Points de terminaison
- Notifications d'événements
- Notifications d'événements par e-mail
- Notifications d'événements par SNS
- Event publishing (Publication d'événement
- FAQ (Questions fréquentes)
- Liste de suppression globale

- Champs d'en-tête, pris en charge
- Identités, gestion
- Gestion des identités et des accès
- Sécurité de l'infrastructure
- Intégration à l'action Amazon WorkMail
- Contrôle basé sur l'IP à l'aide de filtres d'adresses IP
- Action de fonction lambda, invoquer
- Gestion des listes
- Listes et abonnements
- Journalisation et surveillance
- Détection des logiciels malveillants
- Signature DKIM manuelle
- Surveillance de l'envoi d'e-mails à l'aide de la publication d'événements
- Surveillance de la réputation de l'expéditeur
- Surveillance de l'activité d'envoi
- Quotas
- Règles de réception
- Contrôle basé sur le destinataire à l'aide de règles de réception
- Régions
- Métriques de réputation
- Messages des métriques de réputation
- Résilience
- Action du compartiment S3, livrer à
- Environnement de test (sandbox) – sortir de
- Sécurité
- Protocoles de sécurité, pris en charge
- Autorisation d'envoi
- Anatomie de la politique d'autorisation d'envoi
- Exemples de politiques d'autorisation d'envoi
- Processus d'autorisation d'envoi

- Métriques SNDS pour les adresses IP dédiées
- Contenus des notifications SNS
- Exemples de notifications SNS
- Action de rubrique SNS, publier vers
- SPF (Sender Policy Framework) (Cadre de politique de l'expéditeur)
- Arrêt de l'action de jeu de règles
- Gestion des abonnements
- Assistance technique, demander
- Modèles pour la vérification personnalisée des e-mails
- Dépannage
- Identités vérifiées
- Virtual Deliverability Manager
- Points de terminaison d'un VPC

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.