



Guide du développeur

Amazon Simple Email Service



Amazon Simple Email Service: Guide du développeur

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d'Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d'une manière susceptible d'entraîner une confusion chez les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce qu'Amazon SES ?	1
Avantages	1
Services connexes	1
Tarification	2
Régions	2
Régions et terminaux SES	3
Augmentation des limites d'envoi et suppression d'environnement de test (sandbox)	4
Vérification des adresses e-mail et des domaines	4
Easy DKIM	5
Liste de suppression au niveau du compte	5
Notifications de commentaire	5
Informations d'identification SMTP	6
Points de terminaison de commentaires utilisés pour les domaines MAIL FROM personnalisés	6
Autorisation d'envoi	7
Réception d'e-mails	7
Quotas	7
Quotas d'envoi d'e-mails	7
Quotas de réception d'e-mails	12
Quotas du gestionnaire de courrier	13
Quotas généraux	15
Types d'informations d'identification	16
Fonctionnement d'Amazon SES	22
Après l'envoi d'une demande d'e-mail à SES par un expéditeur	23
Après l'envoi d'un e-mail par Amazon SES	24
Format d'e-mail	26
Présentation de la délivrabilité	31
Bonnes pratiques de messagerie électronique	38
Utilisation des AWS SDK	45
Prise en main	47
Configuration	47
Inscrivez-vous pour un Compte AWS	47
Configuration de votre compte SES	47
Téléchargez un AWS SDK (pour utiliser les API SES)	48

Migration vers Amazon SES	48
Étape 1. Vérifier votre domaine	48
Étape 2. Demander un accès de production	49
Étape 3. Configurer les systèmes d'authentification de domaine	49
Étape 4 : Générer vos informations d'identification SMTP	49
Étape 5. Connexion à un point de terminaison SMTP	49
Étapes suivantes	50
Demander un accès de production	50
Limites d'envoi	55
Augmentation de vos quotas d'envoi	57
Augmentation automatique des quotas d'envoi	57
L'utilisateur a demandé des quotas d'envoi supplémentaires	58
Surveillance de vos quotas d'envoi	59
Surveillance de vos quotas d'envoi à l'aide de la console Amazon SES	59
Surveillance de vos quotas d'envoi à l'aide de l'API Amazon SES	60
Erreurs de quotas d'envoi	61
Atteinte des limites d'envoi avec l'API Amazon SES	61
Atteinte des limites d'envoi avec SMTP	61
Configuration de l'envoi d'e-mails	62
Utilisation de l'interface SMTP	62
Conditions requises pour envoyer des e-mails via SMTP	63
Méthodes d'envoi d'e-mails via SMTP	64
Informations à fournir pour les e-mails	64
Obtention des informations d'identification SMTP	64
Connexion à un point de terminaison SMTP	74
Envoi d'e-mails à l'aide de packages logiciels	75
Envoi d'e-mails par programmation	77
Intégration à votre serveur de messagerie existant	87
Test de votre connexion à l'interface SMTP Amazon SES	102
Utilisation de l'API	111
Envoi d'e-mails formatés	112
Envoi d'e-mails bruts	113
Utiliser des modèles pour envoyer des e-mails	125
Envoi d'e-mails à l'aide d'un AWS SDK	150
Encodage de contenu	170
Protocoles de sécurité pris en charge	170

Expéditeur d'e-mails à destination d'Amazon SES	171
Amazon SES à destination d'un récepteur	171
End-to-end chiffrement	172
Champs d'en-tête acceptés	173
Pièces jointes d'e-mail	176
Fonctionnement des pièces jointes	176
Structure de l'objet de fixation	177
Bonnes pratiques	181
Types de pièces jointes non pris en charge	181
Réception d'e-mails	183
Concepts de réception d'e-mails et cas d'utilisation	184
Recipient-based contrôle à l'aide des règles de réception	184
IP-based contrôle à l'aide de filtres d'adresses IP	186
Email-receiving processus	187
Cas d'utilisation & restrictions	188
Authentification d'e-mails et détection de logiciels malveillants	191
Configuration de la réception d'e-mails	192
Vérification de votre domaine	193
Publication d'un registre MX	194
Attribution d'autorisations	197
Instructions pour la console de réception d'e-mails	206
Création de règles de réception	206
Création de filtres d'adresses IP	248
Métriques de réception d'e-mails	250
Locataires - NOUVEAUX	254
Qu'est-ce que la gestion des locataires ?	254
Comment ça marche	255
Association de ressources	255
Surveillance de la réputation	255
Configuration	256
Création de locataires	256
Affectation de ressources	257
Politiques de réputation	258
Envoi d'un e-mail	258
API SendEmail	259
SMTP	260

Statut du locataire	260
État et indicateurs	260
Pause/Unpause	261
Résultats relatifs à la réputation	262
Voir les résultats	262
Compréhension des résultats	263
Résoudre les problèmes	263
Contrôle	264
CloudWatch métriques	264
Notifications EventBridge	265
Confiance et sécurité	267
Bonnes pratiques	268
Listes de suppression	269
Limitations	269
Tarification	270
Identities vérifiées	271
Création et vérification des identités	271
Création d'une identité de domaine	275
Vérification d'une identité de domaine	279
Création d'une identité d'adresse e-mail	286
Vérification d'une identité d'adresse e-mail	287
Créer et vérifier une identité et attribuer un jeu de configuration par défaut en même temps (API)	288
Utilisation de modèles d'e-mail de vérification personnalisé	289
Gestion des identités	302
Afficher les identités à l'aide de la console	303
Supprimer une identité à l'aide de la console	304
Modifier une identité à l'aide de la console	304
Modifier une identité pour utiliser un ensemble de configuration par défaut à l'aide de l'API SES	305
Récupérez le jeu de configuration par défaut utilisé par l'identité à l'aide de l'API SES	307
Remplacer l'ensemble de configuration par défaut actuel utilisé par l'identité à l'aide de l'API SES	307
Configuration des identités	308
Méthodes d'authentification d'e-mail	309
Configuration des notifications d'événement par e-mail	361

Utilisation de l'autorisation d'identité	403
Utilisation de l'autorisation d'envoi	419
Envoi d'e-mails test avec le simulateur	452
Utilisation du simulateur de boîte aux lettres à partir de la console	453
Utilisation manuelle du simulateur de boîte aux lettres	454
Jeux de configurations	459
Créer des jeux de configuration	460
Créer un jeu de configurations	460
Créez un ensemble de configuration (AWS CLI)	466
Gestion des jeux de configurations	467
Afficher, modifier et & supprimer un ensemble de configurations (console)	468
Répertorier les ensembles de configuration (AWS CLI)	468
Obtenez les détails du jeu de configuration (AWS CLI)	469
Supprimer un ensemble de configuration (AWS CLI)	469
Arrêter d'envoyer des e-mails à partir d'un ensemble de configuration (AWS CLI)	469
Comprendre les jeux de configurations par défaut	469
Créer des destination d'événement	471
Attribuer des groupes d'adresses	476
Configurez les domaines personnalisés d'ouverture et de clic	477
Spécification des jeux de configurations dans un e-mail	484
Afficher et exporter des mesures de réputation	484
Activation de l'exportation des mesures de réputation	485
Désactivation de l'exportation des métrique de réputation	485
Points de terminaison globaux	486
Que sont les points de terminaison mondiaux ?	486
Comment fonctionnent les points de terminaison mondiaux	486
Configuration des points de terminaison globaux	487
Conditions préalables	487
Création d'un point de terminaison global	488
États des terminaux mondiaux	488
Préparation de la région secondaire	489
(1) Ensembles de configuration dupliqués	489
(2) Identités de domaine vérifiées dupliquées	490
(3) Limites de production dupliquées	491
Utilisation de points de terminaison globaux	492
Intégration à votre application	493

Surveillance et mesures	494
Bonnes pratiques et considérations	495
Tarification	495
Adresses IP dédiées	497
Configuration simplifiée	499
Gestion de réputation	500
Prévisibilité des envois	500
Volume d'e-mails sortants	501
Coûts supplémentaires	501
Contrôle de la réputation de l'expéditeur	502
Aptitude à isoler la réputation d'expéditeur	502
Adresses IP connues et fixes	502
Standard	503
Demande et abandon	503
Préparation	505
Création de groupes	509
Adresses IP dédiées (gérées)	512
Avantages et fonctionnalités	512
Importance de la préparation	514
FAQ que vous devriez connaître	515
Création d'un groupe d'adresses IP gérées	515
Consultation des métriques d'envoi et de capacité du groupe	519
Suppression d'un groupe d'adresses IP géré	522
Fourniture de vos propres adresses IP	522
Exigences	523
Considérations	523
Utilisation de vos propres adresses IP avec Amazon SES	524
Virtual Deliverability Manager	525
Délivrabilité du SES	526
Prise en main	527
Tableau de bord	530
Conseiller	550
Settings	557
Délivrabilité globale	560
Prise en main	562
Analyse de la campagne	563

Taux de placement des boîtes de réception	564
Tests de placement dans la boîte de réception	565
Listes de blocage	567
Validation par e-mail	569
API de validation des e-mails	570
Validation de l'API (console)	571
Validation de l'API (AWS CLI)	571
Validation automatique	574
Validation automatique (console)	575
Dérogations des ensembles de configuration	576
Validation automatique (AWS CLI)	576
Tableau de bord de validation des e-mails	579
Gestionnaire de courrier	581
Prise en main	582
Prise en main	583
Points de terminaison d'entrée	584
Configuration des points de terminaison d'entrée	585
Rotation des identifiants	591
Politique TLS	592
Authentification mTLS	594
Création d'un point de terminaison d'entrée (console)	595
Politiques de circulation et déclarations de politique	598
Création de politiques de trafic et de déclarations de politique (console)	599
Conditions de la déclaration de politique	601
Ensembles de règles et règles	602
Création d'ensembles de règles et de règles (console)	604
Conditions et actions des règles	606
relais SMTP	611
Création d'un relais SMTP (console)	612
Configuration de Google Workspaces	616
Configuration de Microsoft Office 365	617
Listes d'adresses	620
Que sont les listes d'adresses ?	621
Comment fonctionnent les listes d'adresses	621
Configuration de listes d'adresses	621
Utilisation des listes d'adresses	626

Bonnes pratiques	495
Archivage des e-mails	629
Utilisation de l'archivage des e-mails (console)	630
Compléments par e-mail	635
Abonnement à Add Ons (console)	636
Politiques d'autorisations	638
Politiques relatives aux terminaux d'entrée	638
Politiques de relais SMTP	640
Politiques d'archivage des e-mails	642
Politiques d'action relatives aux règles	646
Logging	654
Configuration de la diffusion des journaux	654
Interprétation des journaux	657
Listes et abonnements	664
Liste de suppression globale	666
Considérations relatives à la liste de suppression globale	667
Utilisation de la liste de suppression au niveau du compte	668
Account-level considérations relatives à la liste de suppression	669
Activation de la liste de suppression au niveau du compte	671
Activation de la liste de suppression au niveau de votre compte pour un jeu de configuration	672
Ajout d'adresses e-mail individuelles à la liste de suppression au niveau de votre compte ...	674
Ajout d'adresses e-mail en bloc à la liste de suppression au niveau de votre compte	676
Affichage d'une liste d'adresses figurant dans la liste de suppression au niveau de votre compte	679
Retrait d'adresses e-mail individuelles de la liste de suppression au niveau de votre compte	682
Retrait d'adresses e-mail en bloc de la liste de suppression au niveau de votre compte	684
Affichage d'une liste de tâches d'importation pour le compte	687
Obtention des informations sur une tâche d'importation pour le compte	689
Désactivation de la liste de suppression au niveau du compte	691
Tenant-level listes de suppression	691
Comment fonctionne la suppression au niveau des locataires	692
Priorité de suppression	693
Enregistrement de suppression automatique	694
Identifier les rebonds liés à la suppression des locataires	695

Gestion des entrées	695
Considérations et restrictions	695
Ressources connexes	696
Configuration de la suppression au niveau du locataire	697
Gestion des entrées de suppression de locataires	705
Utilisation de la de suppression au niveau du jeu de configurations	712
Activer la suppression au niveau du jeu de configurations	715
Utilisation de la gestion des listes	716
Présentation de la gestion des listes	716
Configuration de la gestion des listes	717
Procédure pas à pas de gestion des listes avec des exemples	723
Utilisation de la gestion des abonnements	725
Présentation de la gestion des abonnements	726
Considérations relatives à l'en-tête de désabonnement	727
Ajout d'un lien de pied de page de désabonnement	728
Surveillance de votre activité d'envoi	729
Surveillance à l'aide de la console	735
Tableau de bord du compte	736
Métriques de réputation	737
Paramètres SMTP	738
Utilisation de la console pour l'affichage des métriques	739
Surveiller à l'aide de l'API	741
Appel de l'opération GetSendStatistics d'API à l'aide du AWS CLI	741
Appel de l'opération GetSendStatistics par programmation	742
Surveillance de l'envoi d'e-mails à l'aide de la publication d'événements	745
Comment fonctionne la publication d'événements avec les ensembles de configuration et les balises de message	746
Feedback précis pour les campagnes par e-mail	747
Utilisation de la publication d'événements	748
Terminologie de publication d'événements	749
Configuration de la publication d'événements	750
Utilisation des données d'événement	767
Surveillance de la réputation d'expéditeur	842
Utilisation des métriques de réputation	842
Messages des métriques de réputation	845
Messages de statut général	845

Notification de taux de retours à l'expéditeur	847
Notification de taux de réclamations	849
Notification d'organisation de lutte anti-spam	850
Notification de bombardement de liste	852
Notification de commentaire direct	853
Notification de liste de blocage de domaines	855
Notification de révision en interne	856
Notification de fournisseur de boîte aux lettres	858
Notification de commentaire de destinataires	859
Notification de compte lié	861
Notification de piège pour le courrier indésirable	862
Notification de site vulnérable	863
Notification d'informations d'identification compromises	865
Autre notification	866
Création d'alarmes avec CloudWatch	866
Métriques SNDS pour les applications dédiées IPs	869
Questions relatives au dépannage	871
Interruption automatique d'envoi d'e-mails	872
Pour l'ensemble de votre compte	872
Pour un ensemble de configurations	880
Surveillance à l'aide EventBridge	890
Événements SES	890
Référence du schéma des événements	892
Schéma de statut du conseiller du gestionnaire de délivrabilité virtuel	893
Schéma d'état d'envoi d'e-mails SES	895
En utilisant EventBridge	897
Spécifiez un exemple d'événement dans EventBridge	898
Modèles d'événement pour les événements SES	898
EventBridgeRessources supplémentaires	901
Exemples de code	903
Amazon SES	905
Principes de base	907
Scénarios	1042
API Amazon SES v2	1091
Principes de base	1092
Scénarios	1175

Sécurité	1233
Protection des données	1234
Chiffrement des données au repos	1235
Chiffrement en transit	1247
Suppression de données personnelles	1248
Gestion des identités et des accès	1255
Création de stratégies IAM pour l'accès à SES	1256
Exemples de stratégies IAM pour SES	1260
AWS politiques gérées	1266
Utilisation des rôles liés à un service	1268
Journalisation et surveillance	1271
Journalisation des appels d'API	1272
Validation de conformité	1284
Résilience	1284
Sécurité de l'infrastructure dans SES	1285
Points de terminaison d'un VPC	1285
Exemple de procédure de configuration de SES dans Amazon VPC	1286
Résolution des problèmes	1291
Problèmes généraux	1292
Les modifications que j'apporte ne sont pas visibles immédiatement	1292
Problèmes de vérification	1293
Problèmes de vérification de domaine	1293
Vérification des paramètres de vérification de domaine	1295
Problèmes de vérification d'e-mail	1296
Problèmes liés à la fonction DKIM	1297
Problèmes de remise	1300
Problèmes au niveau des e-mails reçus	1301
Problèmes de notifications	1302
Erreurs d'envoi d'e-mails	1303
Accroissement du débit	1306
Problèmes SMTP	1308
Codes de réponse SMTP	1310
FAQs	1318
DIPS géré FAQs	1318
FAQ sur le DIPS géré, premier trimestre	1318
FAQ sur le DIPS géré, deuxième trimestre	1319

FAQ sur le DIPS géré, 3e trimestre	1319
FAQ sur le DIPS géré, quatrième trimestre	1319
FAQ sur le DIPS géré Q5	1320
FAQ sur le DIPS géré Q6	1320
Processus d'envoi d'avis FAQs	1320
Comptes sous vérification	1321
Suspensions d'envoi	1324
Retours à l'expéditeur	1328
Réclamations	1332
Pièges pour le courrier indésirable	1339
Enquêtes manuelles	1342
Liste DNS Blackhole (DNSBL) FAQs	1344
Q1 FAQ DNSBL	1344
Q2 FAQ DNSBL	1345
Q3 FAQ DNSBL	1345
Q4 FAQ DNSBL	1345
Q5 FAQ DNSBL	1346
Q6 FAQ DNSBL	1347
Métriques relatives aux e-mails FAQs	1348
Général	1349
Suivi des ouvertures	1350
Suivi des clics	1351
Index de recherche rapide	1355
Procédures et concepts	1355
FAQs sur les protocoles pris en charge	1362
Quels sont les protocoles CBOR AWS JSON et Smithy RPC v2, et en quoi diffèrent-ils ?	1362
Comment démarrer avec le protocole CBOR Smithy RPC v2 ?	1362
Quels sont les risques liés à l'activation du protocole CBOR Smithy RPC v2 ?	1363
Et si ma solution ne prend pas en charge Smithy RPC v2 CBOR ?	1363
Quelles AWS régions prennent en charge le protocole CBOR Smithy RPC v2 ?	1363
À quelles améliorations de latence puis-je m'attendre lors de la mise à niveau vers des versions du SDK compatibles avec Smithy RPC v2 CBOR ?	1364
Le protocole AWS JSON sera-t-il obsolète ?	1364
Où puis-je trouver plus d'informations sur Smithy RPC v2 CBOR ?	1364
.....	mccclxv

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 élimine ces difficultés et vous permet de bénéficier des années d'expérience et de l'infrastructure de messagerie Amazon.com sophistiquée conçue pour répondre aux besoins de sa propre clientèle à grande échelle.

Services connexes

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

- 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 [Gestion des identités et des accès AWS\(IAM\)](#).
- 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.
- Utilisez [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

SES est disponible dans plusieurs Régions AWS pays du monde. Dans chaque région, AWS gère 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 de tous les points de terminaison régionaux SES, consultez la section Points de [terminaison et quotas Amazon Simple Email Service](#) dans le. Références générales AWS Pour

en savoir plus sur le nombre de zones de disponibilité disponibles dans chaque région, consultez la section [Infrastructure AWS mondiale](#).

Cette section contient des informations que vous devez connaître si vous envisagez d'utiliser SES en plusieurs fois Régions AWS. Elle traite des sujets suivants :

- [Régions et terminaux 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](#)
- [Points de terminaison de commentaires utilisés pour les domaines MAIL FROM personnalisés](#)
- [Réception d'e-mails](#)
- [Configuration de registres \(MX\)](#)

Pour des informations générales sur Régions AWS, voir les [points AWS de terminaison de service](#) dans la référence AWS générale.

Régions et terminaux SES

Lorsque vous utilisez SES pour envoyer des e-mails, vous vous connectez à une URL qui fournit un point de terminaison pour l'API ou l'interface SMTP de SES. Références générales AWSII contient une liste complète des terminaux que vous utilisez pour envoyer et recevoir des e-mails via SES. Pour plus d'informations, consultez les [points de terminaison et les quotas d'Amazon Simple Email Service](#) Références générales AWS dans les sections spécifiques ci-dessous :

- [Points de terminaison d'API](#) — Lorsque vous envoyez un e-mail via SES, vous pouvez utiliser les points URLs répertoriés dans ce tableau pour envoyer des requêtes HTTPS à l'API SES.
- [Points de terminaison SMTP](#) : vous pouvez utiliser les points URLs répertoriés dans ce tableau pour envoyer des e-mails lorsque vous utilisez l'interface SMTP.
- [Points de terminaison de réception d'e-mails](#) : si vous avez configuré SES pour recevoir les e-mails envoyés à votre domaine, vous pouvez utiliser le point de terminaison SMTP entrant URLs

répertorié dans ce tableau lorsque vous [configurez les enregistrements de l'échangeur de courrier \(MX\) dans les paramètres DNS](#) de votre domaine.

 Note

Les adresses SMTP entrantes URLs 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)

L'état du bac à sable de votre compte peut varier Régions AWS d'un compte à l'autre. En d'autres termes, si votre compte a été supprimé du bac à sable de la région USA Ouest (Oregon), il se peut qu'il se trouve toujours dans le bac à sable de la région USA Est (Virginie du Nord), sauf si vous l'avez également fait supprimer du bac à sable de cette région.

Les limites d'envoi peuvent également être différentes selon le Région AWS. Par exemple, si votre compte est capable d'envoyer 10 messages par seconde dans la région Europe (Irlande), vous pourrez peut-être envoyer plus ou moins de messages dans d'autres régions.

Lorsque vous [soumettez une demande pour que votre compte soit retiré du sandbox](#), ou lorsque vous [soumettez une demande pour que les quotas d'envoi de votre compte soient augmentés](#), assurez-vous de sélectionner tous les éléments Régions AWS auxquels 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 des e-mails via SES, vous devez vérifier que vous possédez bien l'adresse e-mail ou le domaine à partir duquel vous comptez envoyer des e-mails. L'état de vérification des adresses e-mail et des domaines varie également d'un domaine à l'autre Régions AWS. Par exemple, si vous validez 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 exécuter le processus de configuration d'Easy DKIM pour chaque Région AWS endroit où vous souhaitez utiliser Easy DKIM. C'est-à-dire que dans chaque région, vous devez utiliser la console SES ou l'API SES pour générer des enregistrements CNAME. Ensuite, vous devez ajouter tous les enregistrements CNAME à la configuration DNS de votre domaine. Pour en savoir plus sur la configuration d'Easy DKIM, consultez [Easy DKIM dans Amazon SES](#).

Tous n' Régions AWS utilisent pas le domaine DKIM SES par défaut. `dkim.amazonses.com`
Pour voir si votre région utilise un domaine DKIM spécifique à une région, consultez le tableau des [domaines DKIM](#) dans le. Références générales AWS

Liste de suppression au niveau du compte

La liste de suppression au niveau de votre compte SES ne s'applique Compte AWS qu'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 y a deux points importants à noter concernant la configuration de notifications de commentaires multiples Régions AWS :

- Les paramètres d'identité vérifiés, tels que le fait que vous receviez des commentaires par e-mail ou via SNS, ne s'appliquent qu'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 renvoyés via des notifications SNS, vous devez utiliser l'API SES ou la console SES pour configurer les notifications de feedback SNS pour `user@example.com` dans les deux régions.
- Les rubriques SNS que vous utilisez pour le transfert de commentaires doivent se trouver dans la même région que celle où vous utilisez SES.

Pour plus d'informations sur le suivi de votre activité d'envoi par le biais de notifications de commentaires, consultez [Configuration de notifications d'événement pour Amazon SES](#).

Informations d'identification SMTP

Les informations d'identification que vous utilisez pour envoyer des e-mails via l'interface SMTP de SES sont propres à chacun Région AWS. Si vous utilisez l'interface SMTP de 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](#).

Points de terminaison de commentaires utilisés pour les domaines MAIL FROM personnalisés

Si vous utilisez un domaine MAIL FROM personnalisé, 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 pouvez utiliser le même domaine MAIL FROM personnalisé pour les identités vérifiées de manière différente, Régions AWS car les notifications de rebond et de plainte sont envoyées à un point de terminaison de feedback spécifique à la région.

Lorsque vous configurez un domaine MAIL FROM personnalisé, SES indique automatiquement le point de terminaison de feedback approprié pour la région dans laquelle le domaine MAIL FROM personnalisé est configuré. Ce point de terminaison est fourni dans le champ de valeur de l'enregistrement MX pour que vous puissiez le publier (ajouter) à la configuration DNS de votre domaine.

La procédure de configuration MAIL FROM personnalisée est décrite dans [Utilisation d'un domaine MAIL FROM personnalisé](#). À titre de référence, les points de terminaison de feedback que SES utilise pour les différents Régions AWS sont répertoriés dans le tableau des [points de terminaison de feedback](#) du. Références générales AWS

Autorisation d'envoi

Les expéditeurs délégués ne peuvent envoyer des e-mails qu'à partir de l' Région AWS endroit où l'identité du propriétaire 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 SES doivent se trouver dans le même emplacement Région AWS que le point de terminaison SES. Par exemple, si vous utilisez SES dans la région USA Ouest (Oregon), les rubriques SNS, les clés 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 SES au sein d'une région, vous devez créer une règle de réception active définie dans cette région. Les concepts de réception d'e-mails et le processus de configuration sont expliqués dans [Réception d'e-mails avec Amazon SES](#).

Le tableau des [points de terminaison de réception d'e-mails](#) qui figure dans le tableau Références générales AWS répertorie les points de terminaison de réception d'e-mails pour tous ceux Régions AWS où SES prend en charge la réception d'e-mails.

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 .)

Ressource	Quota par défaut	Ajustable
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 supérieurs à 10 Mo sont soumis à une limitation de la bande passante et, en fonction de votre taux d'envoi, vous pouvez être limité à 40MB/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 maximum de locataires	10 000	Oui
Nombre maximal de destinataires par message	50 destinataires par message.  Note Un destinataire correspond à une adresse « To », « CC » ou « BCC ».	Non.
Nombre maximum d'identités que vous pouvez vérifier	10 000 identités par Région AWS.	Veuillez contacter votre gestionnaire de compte AWS pour discuter de votre cas d'utilisation.

Ressource	Quota par défaut	Ajustable
	 Note Une identité est un domaine ou une adresse e-mail que vous utilisez pour envoyer des e-mails via SES.	
Nombre maximum de groupes d'adresses IP dédiées (y compris les groupes d'adresses IP gérées et standard)	50	Non

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

Ressource	Quota par défaut	Ajustable
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
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 ».	Non

i

Note

Le nombre de destinations que vous pouvez contacter en un seul appel de l'API peut être limité par le taux

Ressource	Quota par défaut	Ajustable
	maximal d'envois de votre compte.	

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	500	Non
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	150 Ko	Non

Ressource	Quota par défaut	Ajustable
publiée à l'aide d'une notification Amazon SNS		
Taille maximale des en-têtes d'e-mail pouvant être publiés à l'aide d'une notification Amazon SNS	10 Ko	Non
Taille maximale des en-têtes d'e-mail pouvant être publiés à l'aide d'une fonction AWS Lambda	50 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 points de terminaison d'entrée TLS mutuels	10	Non
Nombre maximal de destinataires par message	100	Non
Taille maximale des e-mails (y compris les en-têtes)	40 Mo	Non

Ressource	Quota par défaut	Ajustable
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	40	Non
Nombre maximum de listes d'adresses par région	100	Non
Nombre maximum d'adresses par liste d'adresses	100 000	Non
Nombre maximum d'ensembles de règles	40	Non
Nombre maximum de règles par ensemble de règles	40	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

Ressource	Quota par défaut	Ajustable
Nombre maximum d'archives actives	10	Non
Nombre maximum de résultats de recherche dans les archives	1 000	Non
Nombre maximal de résultats de recherche d'archives exportés	250 000	Non
Nombre maximum de requêtes de recherche exécutées en parallèle	1	Non
Nombre maximum de demandes d'exportation exécutées 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 <code>SendEmail</code> , <code>SendRawEmail</code> et <code>SendTemplatedEmail</code>)	Non

Ressource	Quota par défaut	Ajustable
	sont limitées à une demande par seconde.	
Parties MIME	500	Non

Quotas divers SES

Ressource	Quota par défaut	Ajustable
Nombre maximum de tâches d'importation simultanées	20	Non
Nombre maximum de tâches d'exportation simultanées	20	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	AWS clés d'accès	ID de clé d'accès et clé d'accès secrète	Consultez Clés d'accès 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
(Vous pouvez accéder à l'API Amazon SES directement ou indirectement via un AWS SDK AWS Command Line Interface , le ou le AWS Tools for Windows PowerShell.)			 Note Pour des raisons de sécurité optimales , utilisez des clés d'accès utilisateur Gestion des identités et des accès AWS (IAM) au lieu de clés d' Compte AWS accès. Vos Compte AWS informations d'identification donnent un accès complet à toutes vos AWS ressources. Vous devez donc les stocker dans un endroit sûr et utiliser les informations d'identification utilisateur IAM pour day-to-day interagir avec AWS elles. Pour de plus amples informations, consultez Informations d'identification du compte racine et informations d'identification de l'utilisateur IAM dans le manuel

Pour accéder à...	Utilisez ces informations d'identification	De quoi sont composées les informations d'identification	Comment obtenir les informations d'identification
			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 root doit s'assurer que la politique de l'utilisateur IAM l'autorise à accéder aux actions IAM suivantes : « iam : », ListUsers « iam : », « iam : CreateUser »

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

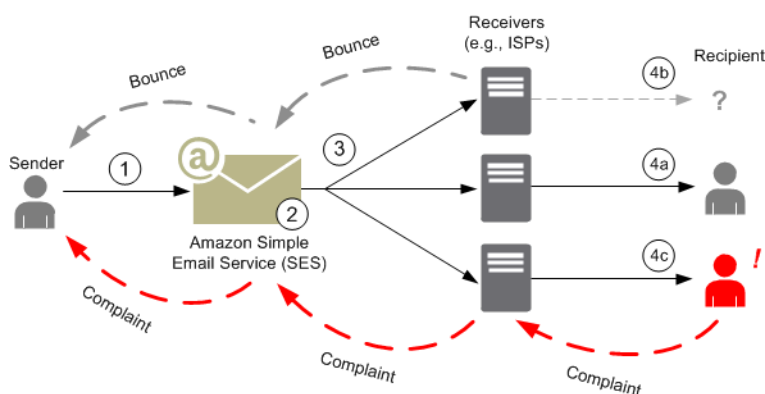
La bonne pratique en matière de sécurité consiste à utiliser un nom d'utilisateur et un mot de passe IAM au lieu d'une adresse e-mail et d'un mot de passe. La combinaison adresse e-mail et mot de passe vous est destinée. Vous devez donc les stocker dans un endroit sûr au lieu de les utiliser pour day-to-day interagir 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 plus d'informations sur les différents types d'informations d'identification de AWS sécurité (à l'exception des informations d'identification SMTP, qui sont utilisées uniquement pour Amazon SES), consultez la section [Informations d'identification AWS de sécurité](#) dans le 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 :
- Le FAI livre avec succès le message dans la boîte de réception du destinataire.
 - 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.
 - 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.

Note

En de rares occasions, SES peut accepter un e-mail de livraison même si la demande d'envoi renvoie une erreur à l'appelant. Si votre application tente à nouveau la demande, un deuxième e-mail avec un identifiant de message différent peut être envoyé, et vous pouvez recevoir des notifications d'événement pour le message associé à l'échec de l'appel. Pour établir une corrélation fiable entre les notifications d'événements et votre logique d'envoi, utilisez des [balises de message](#) plutôt que de vous fier uniquement à l'identifiant du message.

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 AWS SDK pour un langage de programmation qui utilise des exceptions, l'appel à SES lancera un `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 SES-enabled programme n'essaie pas à nouveau d'envoyer des 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 corps et 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. Les destinataires utilisant des clients de messagerie texte auront besoin que vous indiquiez URLs qu'ils peuvent 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 de plus amples informations, veuillez consulter [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 de plus amples informations, veuillez consulter [Envoi d'e-mails bruts à l'aide de l'API Amazon SES v2](#).

Si vous utilisez un AWS SDK pour appeler l'API Amazon SES, vous fournissez les informations répertoriées 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 choisissiez 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 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 : le Sender Policy Framework (SPF) et le courrier DomainKeys identifié (DKIM). Pour de plus amples informations, veuillez consulter [Configuration des identités dans Amazon SES](#).

Quotas d'envoi

Si un fournisseur 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](#).

High-quality courriel

High-quality un e-mail est un e-mail que les destinataires trouvent utile 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 rebonds excessifs, les plaintes et les tentatives d'envoi d'e-mails de mauvaise qualité constituent des abus et vous exposent Compte AWS à un risque de licenciement. 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.

At-least-once livraison

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](#)
- [Maintien d'une bonne réputation d'expéditeur](#)

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 :

- [Retours à l'expéditeur](#)

- [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 associer l'adresse d'un destinataire à une campagne par e-mail en particulier, incluez-en une X-header avec une valeur que vous pouvez retracer jusqu'à 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 identifiants personnalisés X-headers ou spéciaux intégrés dans le corps de l'e-mail afin d'identifier l'adresse e-mail à l'origine de la plainte. 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 prédéfinies. Third-party des services tels que [ReturnPathLitmus](#) peuvent aider à identifier le contenu de votre e-mail susceptible de déclencher des filtres de contenu.
- Si votre e-mail contient des liens, vérifiez les URL de ces liens par rapport aux listes de DNS-based trous noirs (DNSBL), telles que celles trouvées sur et. [URIBL.comSURBL.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.

Maintien d'une bonne réputation d'expéditeur

Dans Amazon SES, la réputation de l'expéditeur fait référence à la crédibilité et à la fiabilité de l'expéditeur de l'e-mail telles que perçues par les fournisseurs de messagerie et les filtres anti-spam. Il s'agit d'une mesure de la probabilité que vos e-mails soient considérés comme légitimes et envoyés avec succès dans les boîtes de réception des destinataires.

Les sections suivantes présentent les principaux principes d'envoi d'e-mails auxquels vous devez prêter attention afin de garantir que vos communications par e-mail atteignent le public cible tout en préservant une bonne réputation d'expéditeur.

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, ne les envoyez pas à partir d'une ISP-based adresse telle que sender@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 de non-réponse, telle que `no-reply@example.com`, comme adresse « De » ou « 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 pour le SPF et le DKIM en envoyant un e-mail à une adresse ISP-based e-mail que vous possédez, telle qu'un compte Gmail ou Hotmail personnel, puis en consultant 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 Kit SDK

AWS des kits de développement logiciel (SDK) sont disponibles pour de nombreux langages de programmation populaires. Chaque kit 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 pour C++	AWS SDK pour C++ exemples de code
AWS CLI	AWS CLI exemples de code
AWS SDK pour Go	AWS SDK pour Go exemples de code
AWS SDK pour Java	AWS SDK pour Java exemples de code
AWS SDK pour JavaScript	AWS SDK pour JavaScript exemples de code
AWS SDK pour Kotlin	AWS SDK pour Kotlin exemples de code
AWS SDK pour .NET	AWS SDK pour .NET exemples de code
AWS SDK pour PHP	AWS SDK pour PHP exemples de code

Documentation SDK	Exemples de code
Outils AWS pour PowerShell	Outils AWS pour PowerShell exemples de code
AWS SDK pour Python (Boto3)	AWS SDK pour Python (Boto3) exemples de code
AWS SDK pour Ruby	AWS SDK pour Ruby exemples de code
AWS SDK pour Rust	AWS SDK pour Rust exemples de code
AWS SDK pour SAP ABAP	AWS SDK pour SAP ABAP exemples de code
AWS SDK pour Swift	AWS SDK pour Swift exemples de code

Pour des exemples spécifiques à Amazon SES, veuillez consulter [Exemples de code pour Amazon SES à l'aide de AWS SDKs](#).

 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 démarrer.

Rubriques

- [Configuration d'Amazon Simple Email Service](#)
- [Migrer vers Amazon SES depuis une autre solution d'envoi d'e-mails](#)
- [Demande d'accès à la production \(sortie du sandbox d'Amazon SES\)](#)

Configuration d'Amazon Simple Email Service

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

Tâches

- [Inscrivez-vous pour un Compte AWS](#)
- [Configuration de votre compte SES](#)
- [Téléchargez un AWS SDK \(pour utiliser les API SES\)](#)

Inscrivez-vous pour un Compte AWS

Pour commencer AWS, vous avez besoin d'un Compte AWS. Pour plus d'informations sur la création d'un Compte AWS, voir [Getting started with an Compte AWS](#) dans le Guide de Gestion de compte AWS référence.

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.

Utilisation de Configuration du compte SES assistant pour configurer 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. 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.

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](#)
- [Étape 2. Demander un accès de production](#)
- [Étape 3. Configurer les systèmes d'authentification de domaine](#)
- [Étape 4 : Générer vos informations d'identification SMTP](#)
- [Étape 5. Connexion à un point de terminaison SMTP](#)
- [Étapes suivantes](#)

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 de plus amples informations, veuillez consulter [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 de plus amples informations, veuillez consulter [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, consultez [Création d'alarmes de surveillance de réputation en utilisant 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 de plus amples informations, veuillez consulter [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 chaque 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 toutes les identités que vous utilisez comme adresses « De », « Source », « Expéditeur » ou Return-Path « ».

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

Tip

- Si vous êtes un nouveau client et que vous n'avez pas encore créé d'identité, l'assistant de configuration du compte SES dans la console sera activé pour vous aider à démarrer. Consultez [Configurer votre compte SES](#) pour savoir comment accéder à l'assistant.
- Si vous avez déjà créé une ou plusieurs identités, vous verrez la page Configurer au lieu de l'assistant de configuration du compte.
 - Si l'une de vos identités est un domaine vérifié, vous pourrez également demander un accès à la production directement depuis la page de configuration. En effet, vérifier votre domaine auprès de SES avant de demander un accès à la production est une bonne pratique qui permet d'obtenir une approbation plus rapide de votre demande d'accès à la production afin que vous puissiez commencer à envoyer des e-mails immédiatement.

Note

- 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 en haut de la console indiquant « Votre compte Amazon SES est dans le bac à sable », sur le côté droit, choisissez Afficher la page de configuration puis Demander un accès à la 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.
 - Marketing email (E-mail marketing) – Envoyé sur une base individuelle vers plusieurs destinataires, à destination d'une liste ciblée de prospects ou de clients avec du contenu marketing et promotionnel, par exemple pour effectuer un achat, télécharger des informations, etc.
 - Transactional email (E-mail transactionnel) – Envoyé individuellement, unique à chaque destinataire, généralement déclenché par une action de l'utilisateur telle qu'un achat de 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. 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.
7. Pour Preferred contact language (Langue de contact préférée), choisissez si vous souhaitez recevoir les communications en English (Anglais) ou Japanese (Japonais).
8. 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.

9. 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 Supportéquipe 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.

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 supprimé du sandbox d'Amazon SES à l'aide du AWS CLI

1. Prérequis : vous devez installer et configurer AWS CLI. Pour plus d'informations, consultez 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 \  
--additional-contact-email-addresses info@example.com \  
--contact-language EN
```

Dans la commande précédente, procédez comme suit :

- a. **TRANSACTIONAL** Remplacez-le par le type d'e-mail que vous prévoyez d'envoyer via Amazon SES. Vous pouvez spécifier TRANSACTIONAL ou MARKETING. 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 *info@example.com* par les adresses e-mail auxquelles 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.
- d. Remplacez *EN* par la langue de votre choix. 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 Supportéquipe 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.

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'acceptation 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 AWS région. Pour plus d'informations sur l'utilisation d'Amazon SES dans plusieurs AWS régions, 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 du sandbox, vous pouvez demander des augmentations de quota supplémentaires à tout moment en créant un nouveau dossier dans le AWS Support Center. Pour de plus amples informations, veuillez consulter [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 `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.

AWS Support SLA d'équipe pour augmenter le nombre de types de demandes

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 console Amazon SES AWS Management Console et ouvrez-la 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).

The screenshot displays the Amazon SES Account dashboard. On the left is a navigation menu with options like 'Account dashboard', 'Reputation metrics', and 'Configuration'. The main content area is titled 'Account dashboard' and includes a 'View reputation metrics' button. It features three main sections: 'Sending limits' (showing a daily quota of 1,000,000 emails and a maximum send rate of 80 emails per second), 'Daily email usage' (showing 345,000 emails sent, 655,000 remaining sends, and 34.50% quota used), and 'Simple Mail Transfer Protocol (SMTP) settings' (listing SMTP endpoint, STARTTLS Port, Transport Layer Security, and TLS Wrapper Port). An 'Account health' section on the right shows the account is 'Healthy'.

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 tentez d'envoyer un e-mail à l'aide de l'API Amazon SES (ou d'un AWS SDK), mais que vous avez déjà dépassé les limites d'envoi de votre compte, l'API génère une `ThrottlingException` erreur. 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 SMTP-enabled logiciel, une application ou un langage de programmation pour envoyer des e-mails via Amazon SES, ou intégrer Amazon SES à votre serveur de messagerie existant, utilisez l'interface SMTP d'Amazon SES. Pour de plus amples informations, veuillez consulter [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 SMTP-enabled programmation et logiciels pour vous connecter à l'interface SMTP d'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 le SMTP-enabled logiciel afin d'envoyer des e-mails via l'interface SMTP d'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. Aucune adresse Reply-To « » que vous spécifiez n'est 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

Pour obtenir la liste des points de terminaison SMTP actuellement disponibles, consultez la section Points de [terminaison SMTP](#) dans le. Références générales AWS

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

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 politique IAM doit vous permettre d'effectuer les actions IAM suivantes :iam:CreateUser,, iam:CreateGroup iam:PutGroupPolicyiam:AddUserToGroup, et. iam:CreateAccessKey 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, une erreur peut s'afficher ou les informations d'identification SMTP peuvent être créées sans les paramètres de stratégie appropriés.

 Important

Certaines des actions IAM référencées ci-dessus, en particulier iam:PutGroupPolicyiam:AddUserToGroup, ont le niveau d'accès à la [gestion des autorisations](#), qui est le niveau IAM le plus élevé, car il donne l'autorisation d'accorder ou de modifier des autorisations de ressources dans le service. Par conséquent, pour améliorer la sécurité de votre AWS compte, il est vivement recommandé de restreindre ou de surveiller régulièrement ces politiques qui incluent la classification des niveaux d'accès à la gestion des autorisations.

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, consultez [Gestion 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 informations d'identification

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

1. Dérivez les informations d'identification SMTP de l'utilisateur à partir de ses AWS informations d'identification en utilisant l'algorithme fourni dans cette section en suivant ces procédures.

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.

2. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à <https://console.aws.amazon.com/iam/> l'adresse.
3. Sous Gestion des accès, sélectionnez Politiques, puis Créer une politique.
4. Dans l'éditeur de politiques, sélectionnez JSON et supprimez tout exemple de code dans l'éditeur.
5. Collez la politique d'autorisation suivante dans l'éditeur :

JSON

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

```
]
}
```

6. Sélectionnez Suivant et entrez AmazonSesSendingAccess dans le champ Nom de la politique, puis Créer une politique.
7. Sous Gestion des accès, sélectionnez Groupes d'utilisateurs, puis Créer un groupe.
8. Entrez AWSSESSendingGroupDoNotRename dans le champ Nom du groupe d'utilisateurs.
9. Ajoutez des utilisateurs SMTP au groupe en les sélectionnant dans le tableau Ajouter des utilisateurs au groupe.
10. Joignez la AmazonSesSendingAccess politique créée précédemment en la sélectionnant dans le tableau Joindre des politiques d'autorisation, puis en cliquant sur Créer un groupe d'utilisateurs.

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 = "wJa1rXUtnFEMI/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.
- Dans l'exemple suivant, la liste de SMTP_REGIONS n'est qu'un exemple : votre liste réelle de régions peut être plus ou moins longue en fonction des régions dans lesquelles vous prévoyez d'envoyer des e-mails, car vous aurez besoin d'informations d'identification SMTP pour chacune d'elles.

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)
"us-gov-east-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/* par le chemin d'accès à l'emplacement où vous avez enregistré `smtp_credentials_generate.py`.
- *wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY* Remplacez-la par la clé d'accès secrète que vous souhaitez convertir en mot de passe SMTP.
- *us-east-1* Remplacez-le par la AWS région dans laquelle vous souhaitez utiliser les informations d'identification SMTP.

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

Migration d'un utilisateur SMTP d'une politique en ligne existante vers une politique de groupe (recommandation de sécurité)

Important

Si vous avez créé des informations d'identification SMTP SES avant le 6 septembre 2024, une politique intégrée et une balise ont été associées à votre utilisateur SMTP. SES s'éloigne

des politiques intégrées et vous encourage à faire de même en tant que recommandation de sécurité.

Avant de migrer un utilisateur SMTP d'une politique en ligne existante vers une stratégie de groupe, vous devez d'abord créer un groupe d'utilisateurs IAM avec la politique d'autorisations SES qui remplacera la politique en ligne. Si vous avez déjà créé ce groupe d'utilisateurs IAM, ou s'il a été créé automatiquement pour les informations d'identification SMTP que vous avez créées à partir du 6 septembre 2024, vous pouvez passer directement à l'étape 10 des procédures suivantes.

Pour migrer d'une politique en ligne existante vers un groupe géré

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à <https://console.aws.amazon.com/iam/> l'adresse.
2. Sous Gestion des accès, sélectionnez Politiques, puis Créer une politique.
3. Dans l'éditeur de politiques, sélectionnez JSON et supprimez tout exemple de code dans l'éditeur.
4. Collez la politique d'autorisation suivante dans l'éditeur :

JSON

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

5. Sélectionnez Suivant et entrez AmazonSesSendingAccess dans le champ Nom de la politique, puis Créer une politique.
6. Sous Gestion des accès, sélectionnez Groupes d'utilisateurs, puis Créer un groupe.
7. Entrez AWSSESSendingGroupDoNotRename dans le champ Nom du groupe d'utilisateurs.
8. Ajoutez des utilisateurs SMTP au groupe en les sélectionnant dans le tableau Ajouter des utilisateurs au groupe.

9. Joignez la `AmazonSesSendingAccess` politique créée précédemment en la sélectionnant dans le tableau Joindre des politiques d'autorisation, puis en cliquant sur Créer un groupe d'utilisateurs.

Maintenant que vous avez créé le groupe d'utilisateurs IAM avec la politique d'autorisations SES, vous pouvez faire migrer un utilisateur SMTP de sa politique en ligne actuelle vers cette stratégie de groupe, comme expliqué dans les étapes restantes.

10. Sous Gestion des accès, choisissez Utilisateurs, puis sélectionnez l'utilisateur SMTP que vous souhaitez migrer.
11. Sélectionnez l'onglet Groupes et choisissez Ajouter un utilisateur aux groupes.
12. Sélectionnez le `AWSSSESSendingGroupDoNotRename` groupe suivi de Ajouter un utilisateur à un ou plusieurs groupes.
13. Sélectionnez l'onglet Autorisations et vérifiez que deux lignes sont répertoriées dans `AmazonSesSendingAccess` la colonne Nom de la politique, l'une avec Inline et l'autre avec Group `AWSSSESSendingGroupDoNotRename` répertorié dans la colonne Attached via.
14. Sélectionnez uniquement la ligne qui figure `AmazonSesSendingAccess` dans la colonne Nom de la politique et Inline dans la colonne Attached via, suivie de Supprimer et de confirmer avec Supprimer la politique.

Vérifiez que la ligne contenant le groupe `AWSSSESSendingGroupDoNotRename` dans la colonne Attached via est conservée.

15. Sélectionnez l'onglet Tags, puis Manage tags.
16. Sélectionnez Supprimer à côté de la ligne figurant `InvokedBy` dans la colonne Clé et `SESConsole` dans la colonne Valeur, puis Enregistrer les modifications.

Important

La `AmazonSesSendingAccess` politique (soit en ligne, soit en tant que stratégie de groupe, soit les deux) doit rester attachée à l'utilisateur SMTP pour s'assurer que son envoi n'est pas impacté. Ne supprimez la politique intégrée qu'une fois que la stratégie de groupe est attachée à votre utilisateur.

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 pour établir une TLS-encrypted connexion : 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 un tel SMTP-enabled logiciel pour envoyer des e-mails via l'interface SMTP d'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 :

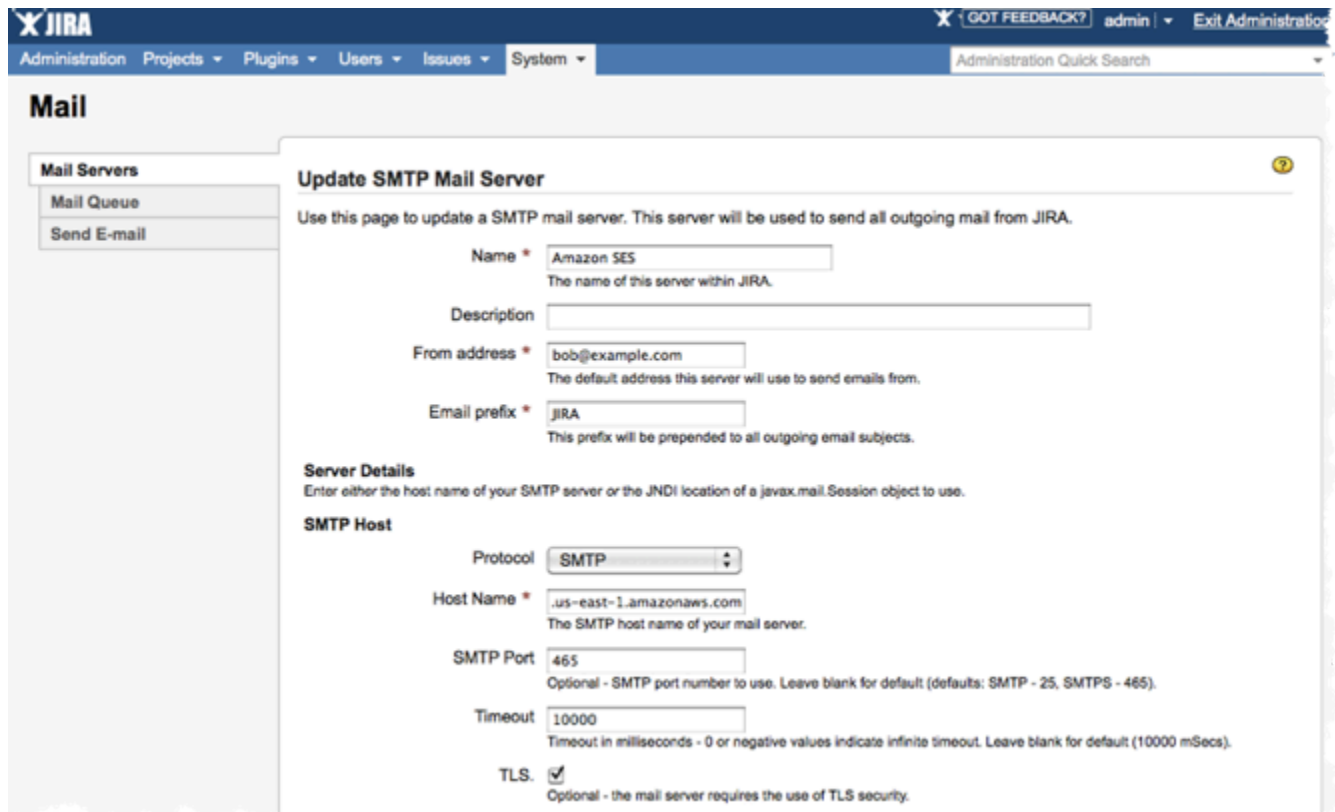
- a. Name (Nom) – Nom descriptif pour ce serveur.
- b. From address (Adresse d'origine) – Adresse à partir de laquelle l'e-mail de retour à l'expéditeur sera envoyé. Vous devez vérifier cette adresse e-mail avec Amazon SES avant de pouvoir l'utiliser pour envoyer des messages. Pour en savoir plus sur 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.



The screenshot shows the JIRA administration interface for configuring email. The 'Mail' section is active, and the 'Update SMTP Mail Server' form is displayed. The form includes fields for Name, Description, From address, Email prefix, SMTP Host (Protocol, Host Name, SMTP Port, Timeout), and TLS. The values entered are: Name: Amazon SES, From address: bob@example.com, Email prefix: JIRA, Protocol: SMTP, Host Name: us-east-1.amazonaws.com, SMTP Port: 465, Timeout: 10000, and TLS is checked.

Mail

Mail Servers

- Mail Queue
- Send E-mail

Update SMTP Mail Server

Use this page to update a SMTP mail server. This server will be used to send all outgoing mail from JIRA.

Name *
The name of this server within JIRA.

Description

From address *
The default address this server will use to send emails from.

Email prefix *
This prefix will be prepended to all outgoing email subjects.

Server Details
Enter either the host name of your SMTP server or the JNDI location of a javax.mail.Session object to use.

SMTP Host

Protocol

Host Name *
The SMTP host name of your mail server.

SMTP Port
Optional - SMTP port number to use. Leave blank for default (defaults: SMTP - 25, SMTPS - 465).

Timeout
Timeout in milliseconds - 0 or negative values indicate infinite timeout. Leave blank for default (10000 mSecs).

TLS. ☒
Optional - the mail server requires the use of TLS security.

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 via l'interface SMTP d'Amazon SES, vous pouvez utiliser un langage de SMTP-enabled programmation, un serveur de messagerie ou une application. 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](#).

Exemples de code

Vous pouvez accéder à l'interface SMTP d'Amazon SES à l'aide d'un langage SMTP-enabled de programmation. Vous fournissez le nom d'hôte et le numéro de port SMTP Amazon SES, ainsi que vos informations d'identification SMTP, puis vous utilisez les fonctions SMTP génériques du langage de programmation pour envoyer l'e-mail.

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'Amazon EC2, vous pouvez demander la suppression de ces restrictions. Pour plus d'informations, consultez [Comment supprimer la restriction sur le port 25 de mon instance ou AWS Lambda fonction Amazon EC2](#) ? dans le AWS Knowledge Center.

Les exemples de code de cette section pour Java et PHP utilisent le port 587 pour éviter ce problème.

Note

Dans ces didacticiels, 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](#).

Sélectionnez un langage de programmation pour afficher l'exemple correspondant à cette langue:

Warning

Amazon SES déconseille d'utiliser des informations d'identification statiques. Reportez-vous [AWS Secrets Manager](#) pour savoir comment améliorer votre niveau de sécurité en supprimant les informations d'identification codées en dur de votre code source. Ce

didacticiel est uniquement fourni dans le but de tester l'interface SMTP d'Amazon SES dans un environnement hors production.

Java

Cet exemple utilise l'[IDE Eclipse](#) et l'[JavaMail API](#) pour envoyer des e-mails via Amazon SES à l'aide de l'interface SMTP.

Avant d'effectuer la procédure suivante, effectuez les tâches dans [Configuration d'Amazon Simple Email Service](#).

Pour envoyer un e-mail à l'aide de l'interface SMTP Amazon SES avec Java

1. Dans un navigateur Web, accédez à la [JavaMail GitHub page](#). Sous Ressources, choisissez javax.mail.jar pour télécharger la dernière version de JavaMail



Important

Ce didacticiel nécessite JavaMail la version 1.5 ou ultérieure. Ces procédures ont été testées à l'aide de JavaMail la version 1.6.1.

2. Dans un navigateur Web, rendez-vous sur la [GitHub page d'activation de Jakarta et, sous JavaBeans Activation Framework 1.2.1 Final Release](#), téléchargez le fichier jakarta.activation.jar
3. Créez un projet Eclipse en procédant comme suit :
 - a. Démarrez Eclipse.
 - b. Dans Eclipse, choisissez File (Fichier), New (Nouveau), puis Java Project.
 - c. Dans la boîte de dialogue Create a Java Project (Créer un projet Java), saisissez un nom de projet, puis choisissez Next (Suivant).
 - d. Dans la boîte de dialogue Java Settings (Paramètres Java), choisissez l'onglet Libraries (Bibliothèques).
 - e. Sélectionnez Classpath et ajoutez les deux fichiers jar externes javax.mail.jar et jakarta.activation.jar à l'aide du bouton Ajouter des fichiers JAR externes.
 - f. Choisissez Add External JARs (Ajouter des JARs externes).
 - g. Accédez au dossier dans lequel vous avez effectué le téléchargement JavaMail. Choisissez le fichier javax.mail.jar, puis Open (Ouvrir).

- h. Dans la boîte de dialogue Java Settings (Paramètres Java), choisissez Finish (Terminer).
4. Dans la fenêtre Package Explorer (Explorateur de paquets) d'Eclipse, développez votre projet.
5. Sous votre projet, cliquez avec le bouton droit sur le répertoire src, puis choisissez New (Nouveau) et Class (Classe).
6. Dans la boîte de dialogue New Java Class (Nouvelle classe Java), dans le champ Name (Nom), entrez AmazonSESSample et choisissez Finish (Terminer).
7. Remplacez la totalité du contenu de AmazonSESSample.java par le code suivant :

```
import java.util.Properties;

import javax.mail.Message;
import javax.mail.Session;
import javax.mail.Transport;
import javax.mail.internet.InternetAddress;
import javax.mail.internet.MimeMessage;

public class AmazonSESSample {

    // Replace sender@example.com with your "From" address.
    // This address must be verified.
    static final String FROM = "sender@example.com";
    static final String FROMNAME = "Sender Name";

    // 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";

    // Replace smtp_username with your Amazon SES SMTP user name.
    static final String SMTP_USERNAME = "smtp_username";

    // The name of the Configuration Set to use for this message.
    // If you comment out or remove this variable, you will also need to
    // comment out or remove the header below.
    static final String CONFIGSET = "ConfigSet";

    // Amazon SES SMTP host name. This example uses the US West (Oregon) region.
    // See https://docs.aws.amazon.com/ses/latest/DeveloperGuide/
    // regions.html#region-endpoints
    // for more information.
    static final String HOST = "email-smtp.us-west-2.amazonaws.com";
```

```
// The port you will connect to on the Amazon SES SMTP endpoint.
static final int PORT = 587;

static final String SUBJECT = "Amazon SES test (SMTP interface accessed
using Java)";

static final String BODY = String.join(
    System.getProperty("line.separator"),
    "<h1>Amazon SES SMTP Email Test</h1>",
    "<p>This email was sent with Amazon SES using the ",
    "<a href='https://github.com/javaee/javamail'>Javamail Package</a>",
    " for <a href='https://www.java.com'>Java</a>."
);

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

    // Create a Properties object to contain connection configuration
    information.
    Properties props = System.getProperties();
    props.put("mail.transport.protocol", "smtp");
    props.put("mail.smtp.port", PORT);
    props.put("mail.smtp.starttls.enable", "true");
    props.put("mail.smtp.auth", "true");

    // Create a Session object to represent a mail session with the
    specified properties.
    Session session = Session.getDefaultInstance(props);

    // Create a message with the specified information.
    MimeMessage msg = new MimeMessage(session);
    msg.setFrom(new InternetAddress(FROM, FROMNAME));
    msg.setRecipient(Message.RecipientType.TO, new InternetAddress(TO));
    msg.setSubject(SUBJECT);
    msg.setContent(BODY, "text/html");

    // Add a configuration set header. Comment or delete the
    // next line if you are not using a configuration set
    msg.setHeader("X-SES-CONFIGURATION-SET", CONFIGSET);

    // Create a transport.
    Transport transport = session.getTransport();

    // Get the password
```

```
String SMTP_PASSWORD = fetchSMTPPasswordFromSecureStorage();

// Send the message.
try
{
    System.out.println("Sending...");

    // Connect to Amazon SES using the SMTP username and password you
    specified above.
    transport.connect(HOST, SMTP_USERNAME, SMTP_PASSWORD);

    // Send the email.
    transport.sendMessage(msg, msg.getAllRecipients());
    System.out.println("Email sent!");
}
catch (Exception ex) {
    System.out.println("The email was not sent.");
    System.out.println("Error message: " + ex.getMessage());
}
finally
{
    // Close and terminate the connection.
    transport.close();
}

static String fetchSMTPPasswordFromSecureStorage() {
    /* IMPLEMENT THIS METHOD */
    // For example, you might fetch it from a secure location or AWS Secrets
    Manager: https://aws.amazon.com/secrets-manager/
}
}
```

8. Dans `AmazonSESSample.java`, remplacez les adresses e-mail suivantes 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 « De ». Vous devez vérifier cette adresse avant d'exécuter ce programme. Pour de plus amples informations, veuillez consulter [Identités vérifiées dans Amazon SES](#).
 - *recipient@example.com*— Remplacez par votre adresse e-mail « À ». Si votre compte est encore dans l'environnement de test (sandbox), vous devez vérifier cette adresse avant de l'utiliser. Pour de plus amples informations, veuillez consulter [Demande d'accès à la production \(sortie du sandbox d'Amazon SES\)](#).
9. AmazonSESSample.java Remplacez les valeurs suivantes par vos propres valeurs :
- *smtp_username*— Remplacez-le par votre identifiant de nom d'utilisateur SMTP. Notez que les informations d'identification de votre nom d'utilisateur SMTP sont une chaîne alphanumérique de 20 caractères, et pas un nom intelligible.
 - *smtp_password*— ``fetchSMTPPasswordFromSecureStorage`` Implémente pour récupérer le mot de passe.
10. (Facultatif) Si vous souhaitez utiliser un point de terminaison SMTP Amazon SES dans un Région AWS autre endroit *email-smtp.us-west-2.amazonaws.com*, remplacez la valeur de la variable par le point HOST de terminaison 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.
11. (Facultatif) – Si vous souhaitez utiliser un jeu de configurations lors de l'envoi de cet e-mail, remplacez la valeur de la variable *ConfigSet* 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](#).
12. Enregistrez AmazonSESSample.java.
13. Pour créer le projet, choisissez Project (Projet), puis Build Project (Créer un projet). (Si cette option est désactivée, cela peut signifier que la génération automatique est activée.)
14. Pour démarrer le programme et envoyer l'e-mail, choisissez Run (Exécuter), puis à nouveau Run (Exécuter).
15. Vérifiez la sortie. Si l'e-mail a été envoyé avec succès, la console affiche « E-mail envoyé ! » Dans le cas contraire, un message d'erreur s'affiche.
16. Connectez-vous au client de messagerie de l'adresse du destinataire. Vous verrez le message que vous avez envoyé.

PHP

Cet exemple utilise la classe PHPMailer pour envoyer des e-mails via Amazon SES à l'aide de l'interface SMTP.

Avant d'effectuer la procédure suivante, effectuez les tâches dans [Configuration d'Amazon Simple Email Service](#). En plus de configurer Amazon SES, vous devez remplir les conditions préalables suivantes pour envoyer des e-mails avec PHP :

Prérequis :

- Installer PHP — PHP est disponible sur <http://php.net/downloads.php>. 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.
- Installation du gestionnaire de dépendances Composer — Après avoir installé le gestionnaire de dépendances Composer, vous pouvez télécharger et installer la classe PHPMailer et ses dépendances. Pour installer Composer, suivez les instructions d'installation sur <https://getcomposer.org/download>.
- Installez la classe PHPMailer — Après avoir installé Composer, exécutez la commande suivante pour installer PHPMailer :

```
path/to/composer require phpmailer/phpmailer
```

Dans la commande précédente, remplacez *path/to/* par le chemin où vous avez installé Composer.

Pour envoyer un e-mail à l'aide de l'interface SMTP Amazon SES avec PHP

1. Créez un fichier nommé `amazon-ses-smtp-sample.php`. Ouvrez le fichier dans un éditeur de texte et collez le code suivant :

```
<?php

// Import PHPMailer classes into the global namespace
// These must be at the top of your script, not inside a function
use PHPMailer\PHPMailer\PHPMailer;
use PHPMailer\PHPMailer\Exception;

// 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';

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

// 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';

// Replace smtp_username with your Amazon SES SMTP user name.
$usernameSmtp = 'smtp_username';

// Specify a configuration set. If you do not want to use a configuration
// set, comment or remove the next line.
$configurationSet = 'ConfigSet';

// If you're using Amazon SES in a region other than US West (Oregon),
// replace email-smtp.us-west-2.amazonaws.com with the Amazon SES SMTP
// endpoint in the appropriate region.
$host = 'email-smtp.us-west-2.amazonaws.com';
$port = 587;

// The subject line of the email
$subject = 'Amazon SES test (SMTP interface accessed using PHP)';

// The plain-text body of the email
$bodyText = "Email Test\r\nThis email was sent through the
    Amazon SES SMTP interface using the PHPMailer class.";

// The HTML-formatted body of the email
$bodyHtml = '<h1>Email Test</h1>
    <p>This email was sent through the
    <a href="https://aws.amazon.com/ses">Amazon SES</a> SMTP
    interface using the <a href="https://github.com/PHPMailer/PHPMailer">
    PHPMailer</a> class.</p>';

$mail = new PHPMailer(true);

try {
    // Specify the SMTP settings.
    $mail->isSMTP();
```

```

$mail->setFrom($sender, $senderName);
$mail->Username    = $usernameSmtp;
$mail->Password    = fetchSMTPPasswordFromSecureStorage();
$mail->Host        = $host;
$mail->Port        = $port;
$mail->SMTPAuth    = true;
$mail->SMTPSecure  = 'tls';
$mail->addCustomHeader('X-SES-CONFIGURATION-SET', $configurationSet);

// Specify the message recipients.
$mail->addAddress($recipient);
// You can also add CC, BCC, and additional To recipients here.

// Specify the content of the message.
$mail->isHTML(true);
$mail->Subject     = $subject;
$mail->Body        = $bodyHtml;
$mail->AltBody     = $bodyText;
$mail->Send();
echo "Email sent!" , PHP_EOL;
} catch (phpmailerException $e) {
    echo "An error occurred. {$e->errorMessage()}", PHP_EOL; //Catch errors from
    PHPMailer.
} catch (Exception $e) {
    echo "Email not sent. {$mail->ErrorInfo}", PHP_EOL; //Catch errors from
    Amazon SES.
}
function fetchSMTPPasswordFromSecureStorage() {
/* IMPLEMENT THIS METHOD */
// For example, you might fetch it from a secure location or AWS Secrets
    Manager: https://aws.amazon.com/secrets-manager/
}

?>

```

2. Dans le fichier `amazon-ses-smtp-sample.php`, remplacez les valeurs suivantes par vos propres valeurs :

- ***sender@example.com***— Remplacez par une adresse e-mail que vous avez vérifiée auprès d'Amazon SES. Pour de plus amples informations, veuillez consulter [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.
- *smtp_username*— Remplacez-le par votre nom d'utilisateur SMTP, que vous avez obtenu sur la page des [paramètres SMTP](#) de la console Amazon SES. Ce n'est pas le même que votre ID de clé d'accès AWS. Notez que les informations d'identification de votre nom d'utilisateur SMTP sont une chaîne alphanumérique de 20 caractères, et pas un nom intelligible.
- *smtp_password*— ``fetchSMTPPasswordFromSecureStorage`` Implémente pour récupérer le mot de passe.
- (Facultatif) *ConfigSet* — Si vous souhaitez utiliser un ensemble de configuration lors de l'envoi de cet e-mail, remplacez cette valeur par le nom du jeu de configuration. Pour en savoir plus sur les jeux de configurations, consultez [Utilisation des jeux de configuration dans Amazon SES](#).
- (Facultatif) *email-smtp.us-west-2.amazonaws.com* — Si vous souhaitez utiliser un point de terminaison SMTP Amazon SES dans une région autre que l'ouest des États-Unis (Oregon), remplacez-le par le point de terminaison SMTP Amazon SES de la région que vous souhaitez utiliser. Pour obtenir la liste des URL des points de terminaison SMTP Régions AWS où Amazon SES est disponible, consultez [Amazon Simple Email Service \(Amazon SES\) dans le. Références générales AWS](#)

3. Enregistrez le fichier `amazon-ses-smtp-sample.php`.
4. Pour exécuter le programme, ouvrez une invite de commande dans le même répertoire que `amazon-ses-smtp-sample.php`, puis tapez `php amazon-ses-smtp-sample.php`.
5. Vérifiez la sortie. Si l'e-mail a été envoyé avec succès, la console affiche « E-mail envoyé ! » Dans le cas contraire, un message d'erreur s'affiche.
6. Connectez-vous au client de messagerie de l'adresse du destinataire. Vous verrez le message que vous avez envoyé.

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 à Postfix](#)
- [Intégration d'Amazon SES à Sendmail](#)
- [Intégration d'Amazon SES au serveur SMTP IIS de Microsoft Windows Server](#)

Intégration d'Amazon SES à Postfix

Postfix est une alternative à l'agent MTA (Message Transfert Agent) de Sendmail couramment utilisé. Pour plus d'informations sur Postfix, rendez-vous sur <http://www.postfix.org> Les procédures présentées dans cette rubrique fonctionnent avec Linux, macOS ou Unix.

Note

Postfix 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.

Conditions préalables

Avant d'exécuter les procédures fournies dans cette section, vous devez effectuer les tâches suivantes :

- Désinstallez l'application Sendmail si elle est installée sur votre système. La procédure d'exécution de cette étape varie en fonction du système d'exploitation que vous utilisez.

⚠ Important

Les références à sendmail suivantes sont liées à la commande Postfix sendmail et non à l'application Sendmail.

- Installez Postfix. La procédure d'exécution de cette étape varie en fonction du système d'exploitation que vous utilisez.
- Installez un package d'authentification SASL. La procédure d'exécution de cette étape varie en fonction du système d'exploitation que vous utilisez. Par exemple, si vous utilisez un RedHat-based système, vous devez installer le `cyrus-sasl-plain` package. Si vous utilisez une Debian ou un Ubuntu-based système, vous devez installer le `libsasl2-modules` paquet.
- Vérifiez l'adresse e-mail ou le domaine que vous utiliserez pour envoyer les e-mails. Pour plus d'informations, consultez [Création d'une identité d'adresse e-mail](#).
- Si votre compte est toujours dans l'environnement de test (sandbox), vous ne pouvez envoyer des e-mails qu'aux adresses e-mail vérifiées. Pour plus d'informations, consultez [Demande d'accès à la production \(sortie du sandbox d'Amazon SES\)](#).

Configuration de Postfix

Terminez la procédure suivante afin de configurer votre serveur de messagerie pour envoyer des e-mails via Amazon SES en utilisant Postfix.

Pour configurer Postfix

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

```
sudo postconf -e "relayhost = [email-smtp.us-west-2.amazonaws.com]:587" \  
"smtp_sasl_auth_enable = yes" \  
"smtp_sasl_security_options = noanonymous" \  
"smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd" \  
"smtp_use_tls = yes" \  
"smtp_tls_security_level = secure" \  
"smtp_tls_note_starttls_offer = yes"
```

 Note

Si vous utilisez Amazon SES dans une AWS région autre que l'ouest des États-Unis (Oregon), remplacez *email-smtp.us-west-2.amazonaws.com* la commande précédente par le point de terminaison SMTP de la région appropriée. Pour de plus amples informations, veuillez consulter [the section called “Régions”](#).

2. Ouvrez le fichier `/etc/postfix/master.cf` dans un éditeur de texte. Recherchez l'entrée suivante :

```
-o smtp_fallback_relay=
```

Si vous recherchez cette entrée, placez-la en commentaire en insérant un caractère `#` (dièse) en début de ligne. Enregistrez et fermez le fichier .

Si cette entrée n'est pas présente, passez à l'étape suivante.

3. Ouvrez le fichier `/etc/postfix/sasl_passwd` dans un éditeur de texte. Si le fichier n'existe pas déjà, créez-le.
4. Ajoutez la ligne suivante à `/etc/postfix/sasl_passwd` :

```
[email-smtp.us-west-2.amazonaws.com]:587 SMTPUSERNAME:SMTPPASSWORD
```

 Note

Remplacez *SMTPUSERNAME* et *SMTPPASSWORD* par vos identifiants de connexion SMTP. Vos informations d'identification de connexion SMTP ne sont pas les mêmes que votre ID de clé d'accès AWS et votre clé d'accès secrète. Pour en savoir plus sur les informations d'identification, consultez [the section called “Obtention des informations d'identification SMTP”](#).

Si vous utilisez Amazon SES dans une AWS région autre que l'ouest des États-Unis (Oregon), remplacez *email-smtp.us-west-2.amazonaws.com* dans l'exemple précédent par le point de terminaison SMTP de la région appropriée. Pour de plus amples informations, veuillez consulter [the section called “Régions”](#).

Enregistrez et fermez `sasl_passwd`.

5. À l'invite de commande, tapez la commande suivante pour créer un fichier de base de données hashmap contenant vos informations d'identification SMTP :

```
sudo postmap hash:/etc/postfix/sasl_passwd
```

6. (Facultatif) Les fichiers `/etc/postfix/sasl_passwd` et `/etc/postfix/sasl_passwd.db` que vous avez créés au cours des étapes précédentes ne sont pas chiffrés. Ces fichiers contenant vos informations d'identification SMTP, nous vous recommandons d'en modifier les autorisations et la propriété afin d'en restreindre l'accès. Pour restreindre l'accès à ces fichiers :

- a. Dans une invite de commande, entrez la commande suivante pour modifier la propriété des fichiers :

```
sudo chown root:root /etc/postfix/sasl_passwd /etc/postfix/sasl_passwd.db
```

- b. Dans une invite de commande, entrez la commande suivante pour modifier les autorisations des fichiers pour que seul l'utilisateur racine puisse lire ou écrire dans ces fichiers :

```
sudo chmod 0600 /etc/postfix/sasl_passwd /etc/postfix/sasl_passwd.db
```

7. Indiquez à Postfix où trouver le certificat d'une autorité de certification (nécessaire pour vérifier le certificat de serveur Amazon SES). La commande que vous utilisez dans cette étape varie en fonction de votre système d'exploitation.

- Si vous utilisez Amazon Linux, Red Hat Enterprise Linux ou une distribution connexe, saisissez la commande suivante :

```
sudo postconf -e 'smtp_tls_CAfile = /etc/ssl/certs/ca-bundle.crt'
```

- Si vous utilisez Ubuntu ou une distribution connexe, saisissez la commande suivante :

```
sudo postconf -e 'smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt'
```

- Si vous utilisez macOS, vous pouvez générer le certificat à partir de l'utilitaire Keychain de votre système. Pour générer le certificat, tapez la commande suivante sur la ligne de commande :

```
sudo security find-certificate -a -p /System/Library/Keychains/  
SystemRootCertificates.keychain | sudo tee /etc/ssl/certs/ca-bundle.crt > /dev/  
null
```

Une fois le certificat généré, tapez la commande suivante :

```
sudo postconf -e 'smtp_tls_CAfile = /etc/ssl/certs/ca-bundle.crt'
```

8. Tapez la commande suivante pour démarrer le serveur Postfix (ou pour recharger les paramètres de configuration si le serveur est déjà en cours d'exécution) :

```
sudo postfix start; sudo postfix reload
```

9. Envoyez un e-mail de test en saisissant ce qui suit sur la ligne de commande, en appuyant sur Entrée après chaque ligne. Remplacez *sender@example.com* par votre adresse e-mail From. L'adresse d'expédition doit être vérifiée pour une utilisation avec Amazon SES. Remplacez *recipient@example.com* par l'adresse de destination. Si votre compte est encore dans l'environnement de test (sandbox), l'adresse du destinataire doit également être vérifiée. Enfin, la dernière ligne du message doit contenir uniquement un point (.), sans autre contenu.

```
sendmail -f sender@example.com recipient@example.com
From: Sender Name <sender@example.com>
Subject: Amazon SES Test
This message was sent using Amazon SES.
.
```

10. Vérifiez la boîte aux lettres associée à l'adresse du destinataire. Si l'e-mail n'arrive pas, vérifiez le dossier des courriers indésirables. Si vous ne trouvez toujours pas l'e-mail, vérifiez le journal de messagerie de votre système (généralement situé dans `/var/log/maillog`) pour en savoir plus.

Exemple d'utilisation avancée

Cet exemple montre comment envoyer un e-mail qui utilise un [ensemble de configuration](#) et qui utilise le MIME-multipart codage pour envoyer à la fois une version en texte brut et une version HTML du message, ainsi qu'une pièce jointe. Il inclut également une [balise de lien](#), qui peut être utilisée pour classer les événements de clic. Le contenu de l'e-mail étant spécifié dans un fichier externe, vous n'avez pas à entrer manuellement les commandes dans la session Postfix.

Pour envoyer un e-mail MIME en plusieurs parties avec Postfix

1. Dans un éditeur de texte, créez un fichier nommé `mime-email.txt`.

2. Dans le fichier texte, collez le contenu suivant, en remplaçant les valeurs en rouge par les valeurs appropriées de votre compte :

```
X-SES-CONFIGURATION-SET: ConfigSet
From: Sender Name <sender@example.com>
Subject: Amazon SES Test
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="YVhZDF1Y2QzMGQ2N2U0YTZmODU"

--YVhZDF1Y2QzMGQ2N2U0YTZmODU
Content-Type: multipart/alternative; boundary="3NjM0N2QwMTE4MWQ0ZTg2NTYxZQ"

--3NjM0N2QwMTE4MWQ0ZTg2NTYxZQ
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

Amazon SES Test

This message was sent from Amazon SES using the SMTP interface.

For more information, see:
http://docs.aws.amazon.com/ses/latest/DeveloperGuide/send-email-smtp.html

--3NjM0N2QwMTE4MWQ0ZTg2NTYxZQ
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

<html>
  <head>
</head>
  <body>
    <h1>Amazon SES Test</h1>
    <p>This message was sent from Amazon SES using the SMTP interface.</p>
    <p>For more information, see
    <a ses:tags="samplekey0:samplevalue0;samplekey1:samplevalue1;"
    href="http://docs.aws.amazon.com/ses/latest/DeveloperGuide/send-email-
smtp.html">
      Using the Amazon SES SMTP Interface to Send Email</a> in the <em>Amazon SES
Developer Guide</em>.</p>
  </body>
</html>
--3NjM0N2QwMTE4MWQ0ZTg2NTYxZQ--
--YVhZDF1Y2QzMGQ2N2U0YTZmODU
```

```
Content-Type: application/octet-stream
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="customers.txt"

SUQsRmlyc3R0YW11LExhc3R0YW11LENvdW50cnkKMzQ4LEpvaG4sU3RpbGVzLENh
bmFkYQo5MjM4OSxKaWUsTGl1LENoaW5hCjczNCxTaGlybGV5LFJvZlZ3VleixV
bm10ZWQgU3RhdGVzCjI4OTMsQW5heWEsSX1lbmdhcixJbmRpYQ==
--YWVhZDF1Y2QzMGMQ2N2U0YTZmODU--
```

Enregistrez et fermez le fichier .

3. Sur la ligne de commande, entrez la commande suivante. Remplacez *sender@example.com* par votre adresse e-mail et remplacez *recipient@example.com* par l'adresse e-mail du destinataire.

```
sendmail -f sender@example.com recipient@example.com < mime-email.txt
```

Si la commande s'exécute correctement, elle se termine sans fournir de sortie.

4. Vérifiez que vous avez bien reçu l'e-mail dans votre boîte de réception. Si le message n'a pas été remis, vérifiez le journal de messagerie dans votre système.

Intégration d'Amazon SES à Sendmail

Sendmail a été lancé au début des années 1980 et a été continuellement amélioré depuis. Il s'agit d'un agent de transfert de messages (Message Transfert Agent, MTA) flexible et configurable avec une grande communauté d'utilisateurs. Sendmail a été racheté par Proofpoint en 2013, mais ce dernier continue à proposer une version open source de Sendmail. Vous pouvez télécharger la [version open source de Sendmail](#) à partir du site web de Proofpoint, ou via un gestionnaire de paquets pour la plupart des distributions Linux.

Les instructions disponibles dans cette section vous expliquent comment configurer Sendmail pour envoyer un e-mail via Amazon SES. Cette procédure a été testée sur un serveur Ubuntu 18.04.2 LTS.

 Note

Sendmail 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.

Conditions préalables

Avant de commencer la procédure décrite dans cette section, vous devez effectuer les étapes suivantes :

- Installez le paquet Sendmail sur votre serveur.

 Note

Selon la distribution du système d'exploitation que vous utilisez, vous devrez peut-être également installer les paquets suivants : `sendmail-cf`, `m4` et `cyrus-sasl-plain`.

- Validez une identité à utiliser pour votre adresse d'expédition. Pour plus d'informations, consultez [Création d'une identité d'adresse e-mail](#).

Si votre compte se trouve dans l'environnement de test (sandbox) Amazon SES, vous devez également valider les adresses auxquelles vous envoyez des e-mails. Pour plus d'informations, consultez [Demande d'accès à la production \(sortie du sandbox d'Amazon SES\)](#).

Si vous utilisez Amazon SES pour envoyer des e-mails à partir d'une instance Amazon EC2, vous devez également effectuer les étapes suivantes :

- Vous devrez peut-être attribuer une adresse IP élastique à votre instance Amazon EC2 pour que les services de messagerie entrante acceptent votre e-mail. Pour plus d'informations, consultez les [adresses IP élastiques Amazon EC2](#) dans le guide de l'utilisateur Amazon EC2.
- 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'Amazon EC2, vous pouvez demander la suppression de ces restrictions. Pour plus d'informations, consultez [Comment supprimer la restriction sur le port 25 de mon instance ou AWS Lambda fonction Amazon EC2 ?](#) dans le AWS Knowledge Center.

Vous pouvez également modifier la procédure de cette section pour utiliser le port 587 plutôt que le port 25.

Configuration de Sendmail

Effectuez les étapes décrites dans cette section pour configurer Sendmail de façon à envoyer des e-mails à l'aide d'Amazon SES.

Important

La procédure décrite dans cette section part du principe que vous souhaitez utiliser Amazon SES dans l'ouest des États-Unis (Oregon) Région AWS. Si vous voulez utiliser une autre région, remplacez toutes les instances `email-smtp.us-west-2.amazonaws.com` dans ces instructions par le point de terminaison SMTP de la région souhaitée. Pour obtenir la liste des URL de points de terminaison SMTP pour Régions AWS où Amazon SES est disponible, consultez [Amazon Simple Email Service \(Amazon SES\)](#) dans le document Références générales AWS.

Pour configurer Sendmail

1. Dans un éditeur de fichier, ouvrez le fichier `/etc/mail/authinfo`. Si le fichier n'existe pas, créez-le.

Ajoutez la ligne suivante à `/etc/mail/authinfo` :

```
AuthInfo:email-smtp.us-west-2.amazonaws.com "U:root" "I:smtpUsername"  
"P:smtpPassword" "M:PLAIN"
```

Dans l'exemple précédent, apportez les modifications suivantes :

- *email-smtp.us-west-2.amazonaws.com* Remplacez-le par le point de terminaison SMTP Amazon SES que vous souhaitez utiliser.
- *smtpUsername* Remplacez-le par votre nom d'utilisateur SMTP Amazon SES.
- *smtpPassword* Remplacez-le par votre mot de passe SMTP Amazon SES.

 Note

Vos identifiants de connexion SMTP sont différents de votre identifiant de clé d'AWS accès et de votre clé d'accès secrète. Pour en savoir plus sur l'obtention de vos informations d'identification de connexion SMTP, consultez [Obtention des informations d'identification SMTP Amazon SES](#).

Lorsque vous avez terminé, enregistrez authinfo.

2. En ligne de commande, entrez la commande suivante pour générer le fichier `/etc/mail/authinfo.db` :

```
sudo sh -c 'makemap hash /etc/mail/authinfo.db < /etc/mail/authinfo'
```

3. En ligne de commande, entrez la commande suivante pour ajouter la prise en charge des relais vers le point de terminaison SMTP Amazon SES.

```
sudo sh -c 'echo "Connect:email-smtp.us-west-2.amazonaws.com RELAY" >> /etc/mail/access'
```

Dans la commande précédente, remplacez *email-smtp.us-west-2.amazonaws.com* par l'adresse du point de terminaison SMTP Amazon SES que vous souhaitez utiliser.

4. Sur la ligne de commande, tapez la commande suivante pour régénérer `/etc/mail/access.db` :

```
sudo sh -c 'makemap hash /etc/mail/access.db < /etc/mail/access'
```

5. En ligne de commande, entrez la commande suivante pour créer des sauvegardes des fichiers `sendmail.cf` et `sendmail.mc` :

```
sudo sh -c 'cp /etc/mail/sendmail.cf /etc/mail/sendmail_cf.backup && cp /etc/mail/sendmail.mc /etc/mail/sendmail_mc.backup'
```

6. Ajoutez les lignes suivantes au fichier `/etc/mail/sendmail.mc` avant toute définition. `MAILER()`

```
define(`SMART_HOST', `email-smtp.us-west-2.amazonaws.com')dn1
define(`RELAY_MAILER_ARGS', `TCP $h 25')dn1
define(`confAUTH_MECHANISMS', `LOGIN PLAIN')dn1
```

```
FEATURE(`authinfo', `hash -o /etc/mail/authinfo.db')dn1
MASQUERADE_AS(`example.com')dn1
FEATURE(masquerade_envelope)dn1
FEATURE(masquerade_entire_domain)dn1
```

Dans le texte précédent, procédez comme suit :

- *email-smtp.us-west-2.amazonaws.com* Remplacez-le par le point de terminaison SMTP Amazon SES que vous souhaitez utiliser.
- *example.com* Remplacez-le par le domaine que vous souhaitez utiliser pour envoyer des e-mails.

Lorsque vous avez terminé, enregistrez le fichier.

 Note

Amazon EC2 limite les communications du port 25 par défaut. Si vous utilisez Sendmail pour envoyer des e-mails à partir d'une instance Amazon EC2, vous devez remplir le [formulaire de demande de suppression des limites d'envoi d'e-mail](#).

7. En ligne de commande, tapez la commande suivante pour rendre sendmail.cf accessible en écriture :

```
sudo chmod 666 /etc/mail/sendmail.cf
```

8. En ligne de commande, tapez la commande suivante pour régénérer sendmail.cf :

```
sudo sh -c 'm4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf'
```

 Note

Si vous rencontrez des erreurs telles que « Commande introuvable » et « Fichier ou répertoire introuvable », assurez-vous que les paquets sendmail-cf et m4 sont installés sur votre système.

9. En ligne de commande, tapez la commande suivante pour réinitialiser les autorisations de sendmail.cf de façon qu'il soit accessible en lecture seule :

```
sudo chmod 644 /etc/mail/sendmail.cf
```

10. En ligne de commande, tapez la commande suivante pour redémarrer Sendmail :

```
sudo /etc/init.d/sendmail restart
```

Selon la version de Linux ou de Sendmail, si ce qui précède ne fonctionne pas, essayez ce qui suit :

```
sudo su service sendmail restart
```

11. Effectuez les étapes suivantes pour envoyer un e-mail de test :

- a. En ligne de commande, entrez la commande suivante.

```
/usr/sbin/sendmail -vf sender@example.com recipient@example.com
```

Remplacez *sender@example.com* par votre adresse e-mail From. Remplacez *recipient@example.com* par l'adresse de destination. Une fois que vous avez terminé, appuyez sur Enter.

- b. Entrez le contenu de message suivant. Appuyez sur Enter à la fin de chaque ligne.

```
From: sender@example.com  
To: recipient@example.com  
Subject: Amazon SES test email
```

```
This is a test message sent from Amazon SES using Sendmail.
```

Lorsque vous avez fini d'entrer le contenu de l'e-mail, appuyez sur Ctrl+D pour l'envoyer.

12. Vérifiez le client du destinataire de l'e-mail pour l'e-mail. Si vous ne trouvez pas l'e-mail, vérifiez le dossier des courriers indésirables. S'il ne s'y trouve pas non plus, vérifiez le journal Sendmail sur votre serveur de messagerie. Le journal se trouve souvent dans `/var/log/mail.log` ou `/var/log/maillog`.

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 rédigées à l'aide de Microsoft Windows Server 2022 sur une instance Amazon EC2. Vous pouvez utiliser la même configuration sur Microsoft Windows Server 2016.

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. Tout d'abord, configurez Microsoft Windows Server 2022 en suivant les instructions suivantes.
 - a. Depuis la [console de gestion Amazon EC2](#), lancez une nouvelle instance Amazon EC2 Microsoft Windows Server 2022 Base.
 - 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. Assurez-vous d'inclure les outils de compatibilité de gestion IIS 10 (une option sous la case à cocher du 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 Outils, choisissez Internet Information Services (IIS) 10.0 Manager.
 - c. Right-click Serveur virtuel SMTP #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 cléAWS 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 terminaux 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 utiliser 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](#).

Conditions préalables

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 d'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 de plus amples informations, veuillez consulter [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 de plus amples informations, veuillez consulter [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'[Test-NetConnection](#) applet de commande pour vous PowerShell 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 pour votre AWS région, puis *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 la ligne de commande pour envoyer un e-mail via l'interface SMTP Amazon SES

Vous pouvez également utiliser la ligne de commande pour envoyer des messages à l'aide de l'interface SMTP Amazon SES. Cette procédure est utile pour tester les informations d'identification SMTP et tester la capacité de destinataires spécifiques à recevoir des messages que vous envoyez via Amazon SES.

Linux, macOS, or Unix

Lorsqu'un expéditeur d'e-mails se connecte à un serveur SMTP, le client émet un ensemble standard de demandes et le serveur répond à chaque demande avec une réponse standard. Cette série de demandes et de réponses est nommée conversation SMTP. Lorsque vous vous connectez au serveur SMTP Amazon SES à l'aide d'OpenSSL, le serveur attend une conversation SMTP.

Lorsque vous utilisez OpenSSL pour vous connecter à l'interface SMTP, vous devez encoder vos informations d'identification SMTP à l'aide de l'encodage base64. Cette section inclut les procédures d'encodage de vos informations d'identification à l'aide de base64.

Pour envoyer un e-mail à partir de la ligne de commande à l'aide de l'interface SMTP

1. Entrez ce qui suit sur la ligne de commande et remplacez-le *email-smtp.us-west-2.amazonaws.com* par l'URL du point de terminaison SMTP Amazon SES pour votre Région AWS. Pour plus d'informations, consultez [the section called “Régions”](#). :

```
#!/bin/bash

# Prompt user to provide following information
read -p "Configuration set: " CONFIGSET
read -p "Enter SMTP username: " SMTPUsername
read -p "Enter SMTP password: " SMTPPassword
read -p "Sender email address: " MAILFROM
read -p "Receiver email address: " RCPT
read -p "Email subject: " SUBJECT
read -p "Message to send: " DATA

echo

# Encode SMTP username and password using base64
EncodedSMTPUsername=$(echo -n "$SMTPUsername" | openssl enc -base64)
EncodedSMTPPassword=$(echo -n "$SMTPPassword" | openssl enc -base64)

# Construct the email
Email="EHLO example.com
AUTH LOGIN
$EncodedSMTPUsername
$EncodedSMTPPassword
MAIL FROM: $MAILFROM
RCPT TO: $RCPT
DATA
X-SES-CONFIGURATION-SET: $CONFIGSET
From: $MAILFROM
To: $RCPT
Subject: $SUBJECT

$DATA
.
QUIT"
```

```
echo "$Email" | openssl s_client -crlf -quiet -starttls smtp -connect email-smtp.us-west-2.amazonaws.com:587
```

2. À l'invite pour chaque variable, entrez vos valeurs.
3. • Pour envoyer en utilisant le protocole SSL implicite sur le port 465, utilisez :

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

Si le message est accepté par Amazon SES, vous voyez une sortie similaire à l'exemple suivant :

```
250 0k 01010160d7de98d8-21e57d9a-JZho-416c-bbe1-8ebaAexample-000000
```

La chaîne de nombres et de texte qui suit 250 0k est l'ID de message de l'e-mail.

 Note

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

PowerShell

Vous pouvez utiliser cette [Net.Mail.SmtpClient](#) classe pour envoyer des e-mails en utilisant un protocole SSL explicite sur le port 587.

 Note

La classe `Net.Mail.SmtpClient` est officiellement obsolète, et Microsoft vous recommande d'utiliser des bibliothèques tierces. Ce code est destiné uniquement à des fins de test et ne doit pas être utilisé pour les charges de travail de production.

Pour envoyer un e-mail PowerShell en utilisant un protocole SSL explicite

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

```
function SendEmail($Server, $Port, $Sender, $Recipient, $Subject, $Body) {
```

```
$Credentials = [Net.NetworkCredential](Get-Credential)

$SMTPClient = New-Object Net.Mail.SmtpClient($Server, $Port)
$SMTPClient.EnableSsl = $true
$SMTPClient.Credentials = New-Object
System.Net.NetworkCredential($Credentials.Username, $Credentials.Password);

try {
    Write-Output "Sending message..."
    $SMTPClient.Send($Sender, $Recipient, $Subject, $Body)
    Write-Output "Message successfully sent to $($Recipient)"
} catch [System.Exception] {
    Write-Output "An error occurred:"
    Write-Error $_
}

}

function SendTestEmail(){
    $Server = "email-smtp.us-west-2.amazonaws.com"
    $Port = 587

    $Subject = "Test email sent from Amazon SES"
    $Body = "This message was sent from Amazon SES using PowerShell (explicit
SSL, port 587)."

$Sender = "sender@example.com"



$Recipient = "recipient@example.com"



SendEmail $Server $Port $Sender $Recipient $Subject $Body



}



SendTestEmail


```

Lorsque vous avez terminé, enregistrez le fichier sous `SendEmail.ps1`.

2. Modifiez le fichier créé lors de l'étape précédente comme suit :

- Remplacez `sender@example.com` par l'adresse e-mail à partir de laquelle vous souhaitez envoyer le message.
- Remplacez `recipient@example.com` par l'adresse e-mail à laquelle vous souhaitez envoyer le message.

- `email-smtp.us-west-2.amazonaws.com` Remplacez-le par l'URL du point de terminaison SMTP Amazon SES de votre AWS région. Pour de plus amples informations, veuillez consulter [Régions et Amazon SES](#).

3. Dans PowerShell, entrez la commande suivante :

```
.\path\to\SendEmail.ps1
```

Dans la commande précédente, remplacez `path\to\SendEmail.ps1` par le chemin du fichier que vous avez créé à l'étape 1.

4. Lorsque vous y êtes invité, entrez votre nom d'utilisateur et votre mot de passe SMTP.

Vous pouvez également utiliser la [System.Web.Mail.SmtpMail](#) classe pour envoyer des e-mails en utilisant le protocole SSL implicite sur le port 465.

Note

La classe `System.Web.Mail.SmtpMail` est officiellement obsolète, et Microsoft vous recommande d'utiliser des bibliothèques tierces. Ce code est destiné uniquement à des fins de test et ne doit pas être utilisé pour les charges de travail de production.

Pour envoyer un e-mail PowerShell en utilisant le protocole SSL implicite

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

```
[System.Reflection.Assembly]::LoadWithPartialName("System.Web") > $null

function SendEmail($Server, $Port, $Sender, $Recipient, $Subject, $Body) {
    $Credentials = [Net.NetworkCredential](Get-Credential)

    $mail = New-Object System.Web.Mail.MailMessage
    $mail.Fields.Add("http://schemas.microsoft.com/cdo/configuration/
smtpserver", $Server)
    $mail.Fields.Add("http://schemas.microsoft.com/cdo/configuration/
smtpserverport", $Port)
    $mail.Fields.Add("http://schemas.microsoft.com/cdo/configuration/
smtpusessl", $true)
    $mail.Fields.Add("http://schemas.microsoft.com/cdo/configuration/
sendusername", $Credentials.UserName)
```

```

    $mail.Fields.Add("http://schemas.microsoft.com/cdo/configuration/
sendpassword", $Credentials.Password)
    $mail.Fields.Add("http://schemas.microsoft.com/cdo/configuration/
smtpconnectiontimeout", $timeout / 1000)
    $mail.Fields.Add("http://schemas.microsoft.com/cdo/configuration/sendusing",
2)
    $mail.Fields.Add("http://schemas.microsoft.com/cdo/configuration/
smtpauthenticate", 1)

    $mail.From = $Sender
    $mail.To = $Recipient
    $mail.Subject = $Subject
    $mail.Body = $Body

    try {
        Write-Output "Sending message..."
        [System.Web.Mail.SmtpMail]::Send($mail)
        Write-Output "Message successfully sent to $($Recipient)"
    } catch [System.Exception] {
        Write-Output "An error occurred:"
        Write-Error $_
    }
}

function SendTestEmail(){
    $Server = "email-smtp.us-west-2.amazonaws.com"
    $Port = 465

    $Subject = "Test email sent from Amazon SES"
    $Body = "This message was sent from Amazon SES using PowerShell (implicit
SSL, port 465)."

    $Sender = "sender@example.com"
    $Recipient = "recipient@example.com"

    SendEmail $Server $Port $Sender $Recipient $Subject $Body
}

SendTestEmail

```

Lorsque vous avez terminé, enregistrez le fichier sous `SendEmail.ps1`.

2. Modifiez le fichier créé lors de l'étape précédente comme suit :

- Remplacez `sender@example.com` par l'adresse e-mail à partir de laquelle vous souhaitez envoyer le message.
 - Remplacez `recipient@example.com` par l'adresse e-mail à laquelle vous souhaitez envoyer le message.
 - `email-smtp.us-west-2.amazonaws.com` Remplacez-le par l'URL du point de terminaison SMTP Amazon SES de votre AWS région. Pour de plus amples informations, veuillez consulter [Régions et Amazon SES](#).
3. Dans PowerShell, entrez la commande suivante :

```
.\path\to\SendEmail.ps1
```

Dans la commande précédente, remplacez `path\to\SendEmail.ps1` par le chemin du fichier que vous avez créé à l'étape 1.

4. Lorsque vous y êtes invité, entrez votre nom d'utilisateur et votre mot de passe SMTP.

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).

- Utilisez 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](#)
- [Envoi d'e-mails bruts à l'aide de l'API Amazon SES v2](#)
- [Utiliser des modèles pour envoyer des e-mails personnalisés à l'aide de l'API Amazon SES](#)
- [Envoi d'e-mails via Amazon SES à l'aide d'un AWS Kit SDK](#)
- [Encodages de contenu pris en charge par Amazon SES](#)

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'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 la construction de messages MIME de courrier électronique bruts

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

SUQsRmlyc3R0YWw1lLExhc3R0YWw1lLENvdW50cnkKMzQ4LEpvaG4sU3RpbGVzLENhbmFkYQo5MjM4
OSxKaWUsTG11LENoaW5hCjczNCxTaGlybGV5LFJvZlJpZ3VleixVbm10ZWQgU3RhdGVzCjI4OTMs
QW5heWEsSX1lbmdhcixJbmRpYQ==

--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 « friendly from », vous devez encoder le nom « friendly from » en utilisant la syntaxe des mots codés MIME, comme décrit dans cette section. 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'opération `SendEmail` Amazon SES API v2, les adresses que vous spécifiez dans les paramètres `Source` et `Destinations` 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 du codage est Q, alors la valeur *encoded-text* doit être utilisée Q-encoding. 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 :

- Q-encoding

```
=?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 plus d'informations sur Q-encoding, consultez la [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 सर्वप्रथम @ च्निह का चयन किया और इनही को ईमेल का आवधिकारक 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 :

```
4KWn4KWv4KWt4KW0I0CkruClhyDgpLDgpYcg4KSf4KWJ4KSu4KSy4KS/4KSC4KS44KSoI0Ckq0Cl
hyDgpKrgpLngpLLgpL4g4KSILeCkruClh+CksiDgpLjgpILgpKbgpYfgpLYg4KSt4KWH4KSc4KS+
IHwg4KS4KWHI0Ckn+ClieCkruCksuKv+CkguCku0CkqCDgpKjgpYcg4KS54KWAIOcku0Cks0Cl
jeCkteCkquCljeCks0CkpeCkriBAIOckmuKv+Ckq0CljeCkuSDgpJXgpL4g4KSa4KSv4KSoI0Ck
leCkv+Ckr+CkviDgpJTgpLAG4KSH4KSo4KWN4KS54KWAIOckleCliyDgpIjgpK7gpYfgpLIg4KSV
4KS+IOckhuCkteCkv+Ckt+CljeCkleCkvuCks0CklSDgpK7gpL7gpKjgpL4g4KSc4KS+4KSk4KS+
IOckueCliAo=
```

 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 Content-Type déclarations 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 manière 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 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 SES non pris en charge](#).

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

L'API Amazon SES v2 fournit l'SendMessageAction, 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 modèle. 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 [JavaMail](#) bibliothèque et [AWS SDK pour Java](#) comment 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 pour 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!");
} catch (Exception ex) {
    // Display an error if something goes wrong.
    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 pour Python \(Boto\)](#) pour composer et envoyer un e-mail brut.

```

import json
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
import os

def boto3_rawemailv2():
    SENDER = "Sender <sender@example.com>"
    RECIPIENT = "recipient@example.com"
    CONFIGURATION_SET = "ConfigSet"
    AWS_REGION = "us-east-1"
    SUBJECT = "Customer service contact info"
    ATTACHMENT = "path/to/customers-to-contact.xlsx"
    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/>
<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"
    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)
msg.attach(att)

#changes start from here
strmsg = str(msg)
body = bytes (strmsg, 'utf-8')

client = boto3.client('sesv2')
response = client.send_email(
    FromEmailAddress=SENDER,
    Destination={
        'ToAddresses': [RECIPIENT]
    },
    Content={
        'Raw': {
            'Data': body
```

```
    }  
  }  
)  
print(response)  
boto3_rawemailv2 ()
```

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

Dans Amazon SES, vous pouvez envoyer un modèle d'e-mail en utilisant un modèle enregistré ou en utilisant un modèle intégré.

- **Modèle stocké** : fait référence à la [Template](#) ressource créée et enregistrée dans SES à l'aide de l'`CreateEmailTemplate` opération de l'API Amazon SES v2. Le modèle contient l'objet et le corps de l'e-mail contenant des variables (espaces réservés) conformes au contenu écrit. Le nom du modèle stocké et les données dynamiques associées aux variables d'espace réservé du modèle sont fournis lors de l'appel des opérations d'API `SendEmail` ou de l'API `SendBulkEmail` v2.

Les modèles enregistrés peuvent être facilement réutilisés et peuvent vous faire économiser du temps et des efforts lors de l'envoi de types d'e-mails similaires. Au lieu de créer chaque e-mail à partir de zéro, il vous suffit de créer la structure de base et le design une seule fois, puis de simplement mettre à jour le contenu dynamique du modèle.

- **Modèle intégré** — La `Template` ressource n'est pas utilisée, mais l'objet et le corps de l'e-mail contenant des variables (espaces réservés) intégrés au contenu écrit, ainsi que les valeurs de ces variables d'espace réservé, sont fournis lors de l'appel des opérations de l'API `SendEmail` ou `SendBulkEmail` de l'API v2.

Les modèles intégrés rationalisent le processus d'envoi d'e-mails en masse en éliminant le besoin de gérer les ressources des modèles dans votre compte SES et simplifient le processus d'intégration en vous permettant d'inclure le contenu du modèle directement dans la logique de votre application. Ils ne sont pas pris en compte dans la limite de 20 000 modèles par Région AWS.

Les limites suivantes s'appliquent lors de l'utilisation de modèles enregistrés :

- 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.

La limite suivante s'applique lors de l'utilisation de modèles intégrés :

- La taille de chaque fichier JSON d'entrée peut atteindre 1 Mo, y compris les parties texte et HTML.

Ce qui suit s'applique à la fois aux modèles stockés et aux modèles en ligne :

- Il n'y a aucune limite quant au nombre de variables de remplacement pouvant être utilisées.
- Vous pouvez envoyer un e-mail à un maximum de 50 objets de destination lors de chaque appel à l'opération `SendBulkEmail`. L'objet `Destination` peut contenir plusieurs destinataires définis dans `ToAddresses`, `CcAddresses`, et `BccAddresses`. Le nombre de destinations que vous pouvez contacter en un seul appel à l'API v2 peut être limité par le taux d'envoi maximal de votre compte. Pour de plus amples informations, veuillez consulter [Gestion de vos limites d'envoi Amazon SES](#).

Ce chapitre inclut des procédures avec des exemples d'utilisation à la fois de modèles stockés et de modèles intégrés.

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](#).

(Facultatif) Partie 1 : Configuration des notifications d'événements d'échec de rendu

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. C'est pourquoi, si vous envisagez d'envoyer un e-mail personnalisé, vous devez configurer SES pour envoyer des notifications d'échec de rendu 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.

(Facultatif) Partie 2 : Création d'un modèle d'e-mail

Si vous avez l'intention d'utiliser un modèle stocké, cette section explique comment utiliser l'opération API [CreateEmailTemplate](#) SES v2 pour créer le modèle. Vous pouvez ignorer cette étape si vous souhaitez utiliser un modèle intégré.

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 nouveau fichier et collez le code suivant en le personnalisant selon vos besoins.

```
{
  "TemplateName": "MyTemplate",
  "TemplateContent": {
    "Subject": "Greetings, {{name}}!",
    "Text": "Dear {{name}},\r\nYour favorite animal is {{favoriteanimal}}.",
    "Html": "<h1>Hello {{name}},</h1><p>Your favorite animal is
{{favoriteanimal}}.</p>"
  }
}
```

Ce code contient les propriétés suivantes :

- **TemplateName**— Le nom de la Template ressource. Lorsque vous envoyez l'e-mail, vous faites référence à ce nom.

- **TemplateContent**— Un conteneur pour les attributs suivants :
 - **Objet** : 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.
 - **Html** — Le corps HTML de l'e-mail. Cette propriété peut contenir des balises de remplacement. L'exemple précédent contient deux balises : `{{name}}` et `{{favoriteanimal}}`.
 - **Texte** : corps du texte de l'e-mail. Les destinataires dont les clients de messagerie n'affichent pas de contenu HTML verront cette version de l'e-mail. Cette propriété peut également contenir des étiquettes 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, tapez la commande suivante pour créer un nouveau modèle à l'aide de l'opération d'API [CreateEmailTemplatev2](#) :

```
aws sesv2 create-email-template --cli-input-json file://mytemplate.json
```

Partie 3 : Envoi de l'e-mail personnalisé

Vous pouvez utiliser les deux opérations d'API SES v2 suivantes pour envoyer des e-mails à l'aide de modèles stockés ou de modèles intégrés :

- L'[SendEmail](#) opération est utile pour envoyer un e-mail personnalisé à un seul objet de destination. L'[Destination](#) objet API v2 peut contenir les `BccAddresses` propriétés `ToAddresses` `CcAddresses`, et. Ils peuvent être utilisés dans n'importe quelle combinaison et peuvent contenir une ou plusieurs adresses e-mail qui recevront le même e-mail.
- L'[SendBulkEmail](#) opération est utile pour envoyer des e-mails uniques à plusieurs objets de destination en un seul appel à l'API v2.

Cette section fournit des exemples d'utilisation du modèle AWS CLI d'e-mail à l'aide de ces deux opérations d'envoi.

Envoi d'un modèle d'e-mail à un seul objet de destination

Vous pouvez utiliser cette [SendEmail](#) opération pour envoyer un e-mail à un ou plusieurs destinataires définis dans un seul objet de destination. Toutes les destinataires de l'objet [Destination](#) recevront le même e-mail.

Pour envoyer un modèle d'e-mail à un seul objet de destination

1. Selon que vous souhaitez utiliser un modèle enregistré ou un modèle intégré, sélectionnez l'exemple de code correspondant à coller dans un éditeur de texte, en le personnalisant selon vos besoins.

Stored template code example

Notez que le modèle que vous avez créé à l'[MyTemplate](#) étape précédente est référencé comme valeur du `TemplateName` paramètre.

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

Ce code contient les propriétés suivantes :

- **FromEmailAddress**— L'adresse e-mail de l'expéditeur.
- **Destination** : objet contenant les destinataires des e-mails définis dans les `BccAddresses` propriétés `ToAddresses` `CcAddresses`, et. Ils peuvent être utilisés dans n'importe quelle combinaison et peuvent contenir une ou plusieurs adresses e-mail qui recevront le même e-mail.

- **TemplateName**— Le nom de la Template ressource à appliquer à l'e-mail.
- **TemplateData**— Chaîne JSON échappée contenant des paires clé-valeur. Les clés correspondent aux variables définies dans les TemplateContent propriétés du modèle stocké, par exemple `{{name}}`. Les valeurs représentent le contenu qui remplace les variables.
- **ConfigurationSetName**— Le 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 de plus amples informations, veuillez consulter [the section called “\(Facultatif\) Partie 1 : Configuration des notifications”](#).

Inline template code example

Notez que les TemplateContent propriétés (qui seraient normalement définies dans un modèle stocké) sont définies en ligne avec la TemplateData propriété qui en fait un modèle en ligne.

```
{
  "FromEmailAddress": "Mary Major <mary.major@example.com>",
  "Destination": {
    "ToAddresses": [
      "alejandro.rosalez@example.com", "jimmy.jet@example.com"
    ]
  },
  "Content": {
    "Template": {
      "TemplateContent": {
        "Subject": "Greetings, {{name}}!",
        "Text": "Dear {{name}},\r\nYour favorite animal is {{favoriteanimal}}.",
        "Html": "<h1>Hello {{name}},</h1><p>Your favorite animal is {{favoriteanimal}}.</p>"
      },
    },
  },
}
```

```
    "TemplateData": "{ \"name\": \"Alejandro\", \"favoriteanimal\":  
    \"alligator\" }"  
    },  
    "ConfigurationSetName": "ConfigSet"  
}
```

Ce code contient les propriétés suivantes :

- **FromEmailAddress**— L'adresse e-mail de l'expéditeur.
- **Destination** : objet contenant les destinataires des e-mails définis dans les `BccAddresses` propriétés `ToAddresses` `CcAddresses`, et. Ils peuvent être utilisés dans n'importe quelle combinaison et peuvent contenir une ou plusieurs adresses e-mail qui recevront le même e-mail.
- **TemplateContent**— Un conteneur pour les attributs suivants :
 - **Objet** : 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.
 - **Html** — Le corps HTML de l'e-mail. Cette propriété peut contenir des balises de remplacement. L'exemple précédent contient deux balises : `{{name}}` et `{{favoriteanimal}}`.
 - **Texte** : corps du texte de l'e-mail. Les destinataires dont les clients de messagerie n'affichent pas de contenu HTML verront cette version de l'e-mail. Cette propriété peut également contenir des étiquettes de remplacement.
- **TemplateData**— Chaîne JSON échappée contenant des paires clé-valeur. Les clés correspondent aux variables définies dans les `TemplateContent` propriétés de ce fichier, par exemple `{{name}}`. Les valeurs représentent le contenu qui remplace les variables.
- **ConfigurationSetName**— Le 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 de plus amples informations, veuillez consulter [the section called “\(Facultatif\) Partie 1 : Configuration des notifications”](#).

2. Personnalisez l'exemple précédent pour l'adapter à vos besoins, puis enregistrez le fichier sous *myemail.json*.
3. Sur la ligne de commande, tapez la commande API v2 suivante pour envoyer l'e-mail :

```
aws sesv2 send-email --cli-input-json file://myemail.json
```

Envoi d'un modèle d'e-mail à plusieurs objets de destination

Vous pouvez utiliser cette [SendBulkEmail](#) opération pour envoyer un e-mail à plusieurs objets de destination en un seul appel à l'API SES v2. SES envoie un e-mail unique au ou aux destinataires de chaque [Destination](#) objet.

Pour envoyer un modèle d'e-mail à plusieurs objets de destination

1. Selon que vous souhaitez utiliser un modèle enregistré ou un modèle intégré, sélectionnez l'exemple de code correspondant à coller dans un éditeur de texte, en le personnalisant selon vos besoins.

Stored template code example

Notez que le modèle que vous avez créé à l'*MyTemplate* étape précédente est référencé comme valeur du *TemplateName* paramètre.

```
{
  "FromEmailAddress": "Mary Major <mary.major@example.com>",
  "DefaultContent": {
    "Template": {
      "TemplateName": "MyTemplate",
      "TemplateData": "{ \"name\": \"friend\", \"favoriteanimal\": \"unknown\" }"
    }
  },
  "BulkEmailEntries": [
    {
      "Destination": {
        "ToAddresses": [
          "anaya.iyengar@example.com"
        ]
      },
      "ReplacementEmailContent": {
```

```

        "ReplacementTemplate": {
            "ReplacementTemplateData": "{ \"name\": \"Anaya\",
\"favoriteanimal\": \"angelfish\" }"
        }
    },
    {
        "Destination": {
            "ToAddresses": [
                "liu.jie@example.com"
            ]
        },
        "ReplacementEmailContent": {
            "ReplacementTemplate": {
                "ReplacementTemplateData": "{ \"name\": \"Liu\",
\"favoriteanimal\": \"lion\" }"
            }
        }
    },
    {
        "Destination": {
            "ToAddresses": [
                "shirley.rodriguez@example.com"
            ]
        },
        "ReplacementEmailContent": {
            "ReplacementTemplate": {
                "ReplacementTemplateData": "{ \"name\": \"Shirley\",
\"favoriteanimal\": \"shark\" }"
            }
        }
    },
    {
        "Destination": {
            "ToAddresses": [
                "richard.roe@example.com"
            ]
        },
        "ReplacementEmailContent": {
            "ReplacementTemplate": {
                "ReplacementTemplateData": "{}"
            }
        }
    }
}

```

```
    ],  
    "ConfigurationSetName": "ConfigSet"  
  }  
}
```

Ce code contient les propriétés suivantes :

- **FromEmailAddress**— L'adresse e-mail de l'expéditeur.
- **DefaultContent**— Un objet JSON contenant les **TemplateData** objets **TemplateName** et.
- **TemplateName**— Le nom de la **Template** ressource à appliquer à l'e-mail.
- **TemplateData**— Contient des paires clé-valeur qui seront utilisées si l'**ReplacementEmailContent**objet contient un objet JSON vide dans la **ReplacementTemplateData** propriété. {}
- **BulkEmailEntries**— Tableau contenant un ou plusieurs **Destination** objets.
- **Destination** : objet contenant les destinataires des e-mails définis dans les **BccAddresses**propriétés **ToAddresses****CcAddresses**, et. Ils peuvent être utilisés dans n'importe quelle combinaison et peuvent contenir une ou plusieurs adresses e-mail qui recevront le même e-mail.
- **ReplacementTemplateData**— 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. (Si la chaîne JSON est vide, indiquée par {}, les paires clé-valeur définies dans la **TemplateData** propriété de l'**DefaultContent**objet seront utilisées.)
- **ConfigurationSetName**— Le 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 de plus amples informations, veuillez consulter [the section called “\(Facultatif\) Partie 1 : Configuration des notifications”](#).

Inline template code example

Notez que les `TemplateContent` propriétés (qui seraient normalement définies dans un modèle stocké) sont définies en ligne avec la `TemplateData` propriété qui en fait un modèle en ligne.

```
{
  "FromEmailAddress": "Mary Major <mary.major@example.com>",
  "DefaultContent": {
    "Template": {
      "TemplateContent": {
        "Subject": "Greetings, {{name}}!",
        "Text": "Dear {{name}},\r\nYour favorite animal is
{{favoriteanimal}}.",
        "Html": "<h1>Hello {{name}},</h1><p>Your favorite animal is
{{favoriteanimal}}.</p>"
      },
      "TemplateData": "{ \"name\": \"friend\", \"favoriteanimal\": \"unknown
\" }"
    }
  },
  "BulkEmailEntries": [
    {
      "Destination": {
        "ToAddresses": [
          "anaya.iyengar@example.com"
        ]
      },
      "ReplacementEmailContent": {
        "ReplacementTemplate": {
          "ReplacementTemplateData": "{ \"name\": \"Anaya\",
\"favoriteanimal\": \"angelfish\" }"
        }
      }
    },
    {
      "Destination": {
        "ToAddresses": [
          "liu.jie@example.com"
        ]
      }
    }
  ]
}
```

```

        "ReplacementEmailContent": {
            "ReplacementTemplate": {
                "ReplacementTemplateData": "{ \"name\": \"Liu\",
\"favoriteanimal\": \"lion\" }"
            }
        },
        {
            "Destination": {
                "ToAddresses": [
                    "shirley.rodriguez@example.com"
                ]
            },
            "ReplacementEmailContent": {
                "ReplacementTemplate": {
                    "ReplacementTemplateData": "{ \"name\": \"Shirley\",
\"favoriteanimal\": \"shark\" }"
                }
            }
        },
        {
            "Destination": {
                "ToAddresses": [
                    "richard.roe@example.com"
                ]
            },
            "ReplacementEmailContent": {
                "ReplacementTemplate": {
                    "ReplacementTemplateData": "{}"
                }
            }
        }
    ],
    "ConfigurationSetName": "ConfigSet"
}

```

Ce code contient les propriétés suivantes :

- **FromEmailAddress**— L'adresse e-mail de l'expéditeur.
- **DefaultContent**— Un objet JSON contenant les **TemplateData** objets **TemplateContent** et.
- **TemplateContent**— Un conteneur pour les attributs suivants :

- **Objet** : 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.
- **Html** — Le corps HTML de l'e-mail. Cette propriété peut contenir des balises de remplacement. L'exemple précédent contient deux balises : `{{name}}` et `{{favoriteanimal}}`.
- **Texte** : corps du texte de l'e-mail. Les destinataires dont les clients de messagerie n'affichent pas de contenu HTML verront cette version de l'e-mail. Cette propriété peut également contenir des étiquettes de remplacement.
- **TemplateData**— Contient des paires clé-valeur qui seront utilisées si l'`ReplacementEmailContentobjet` contient un objet JSON vide dans la `ReplacementTemplateData` propriété. `{}`
- **BulkEmailEntries**— Tableau contenant un ou plusieurs `Destination` objets.
- **Destination** : objet contenant les destinataires des e-mails définis dans les `BccAddresses` propriétés `ToAddresses` `CcAddresses`, et. Ils peuvent être utilisés dans n'importe quelle combinaison et peuvent contenir une ou plusieurs adresses e-mail qui recevront le même e-mail.
- **ReplacementTemplateData**— Chaîne JSON échappée contenant des paires clé-valeur. Les clés correspondent aux variables définies dans les `TemplateContent` propriétés de ce fichier, par exemple `{{name}}`. Les valeurs représentent le contenu qui remplace les variables de l'e-mail. (Si la chaîne JSON est vide, indiquée par `{}`, les paires clé-valeur définies dans la `TemplateData` propriété de l'`DefaultContentobjet` seront utilisées.)
- **ConfigurationSetName**— Le 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 de plus amples informations, veuillez consulter [the section called “\(Facultatif\) Partie 1 : Configuration des notifications”](#).

2. Modifiez les valeurs dans le code ci-dessus selon vos besoins, puis enregistrez le fichier sous le nom *mybulkemail.json*.
3. Sur la ligne de commande, tapez la commande API v2 suivante pour envoyer l'e-mail en masse :

```
aws sesv2 send-bulk-email --cli-input-json file://mybulkemail.json
```

Personnalisation avancée des e-mails

Si vous utilisez un modèle stocké, c'est-à-dire que vous avez créé une [Template](#) ressource dans Amazon SES à l'aide de l'CreateEmailTemplateAPI SES v2, vous pouvez tirer parti du système Handlebars pour créer des modèles qui incluent des fonctionnalités avancées, telles que des attributs imbriqués, l'itération de tableaux, des instructions conditionnelles de base et la création de partiels intégrés. 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, consultez [Built-InHelpers](#) at 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](#)
- [Itération au moyen de listes](#)
- [Utilisation des instructions conditionnelles de base](#)
- [Création de fichiers partiels en ligne](#)

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/preferences/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/preferences/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 `SendEmail` ou `SendBulkEmail` 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 `SendBulkEmail`, 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/preferences/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/preferences/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/preferences/i.aspx?
id={{meta.userId}}.
        {{else}}
        Please update your subscription preferences by visiting the
        Preference Center at https://www.example.com/preferences/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 :

Your Preferences

Dear Shirley,

Please update your subscription preferences by visiting the [Preference Center](#).

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

Outre la [création de modèles d'e-mail](#), vous pouvez également utiliser l'API Amazon SES v2 pour mettre à jour ou supprimer des modèles existants, pour répertorier tous vos modèles existants ou pour afficher le contenu d'un modèle.

Cette section contient les procédures d'utilisation du AWS CLI pour effectuer des tâches liées aux modèles 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 le fonctionnement de l'API [ListEmailTemplate](#) SES v2 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 sesv2 list-email-templates
```

S'il existe des modèles d'e-mail dans votre compte 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'opération API [GetEmailTemplate](#) SES v2 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 sesv2 get-email-template --template-name MyTemplate
```

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

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

Suppression d'un modèle d'e-mail

Vous pouvez utiliser l'opération API [DeleteEmailTemplate](#) SES v2 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 sesv2 delete-email-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 [GetTemplate](#) opération.

Mise à jour d'un modèle d'e-mail

Vous pouvez utiliser l'opération API [UpdateEmailTemplate](#) SES v2 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

- Utilisez la commande `GetEmailTemplate` pour récupérer le modèle existant en entrant la commande suivante sur la ligne de commande :

```
aws sesv2 get-email-template --template-name MyTemplate
```

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

Si le nom du modèle que vous avez fourni correspond à un modèle existant dans votre compte 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\nthe 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 sesv2 update-email-template --cli-input-json file://path/to/  
update_template.json
```

Dans la commande précédente, remplacez *path/to/update_template.json* par le chemin du `update_template.json` fichier 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 en utilisant cette [GetEmailTemplate](#) opération.

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 Kit SDK

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

Conditions préalables

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 de plus amples informations, veuillez consulter [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 Kit 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 pour .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 AWSSDK.Core package (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 pour .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. Program.cs Dans l'onglet, 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 pour .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 pour .NET.";

        // The HTML body of the email.
        static readonly string htmlBody = @"<html>
<head></head>
<body>
    <h1>Amazon SES Test (SDK pour .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 pour .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.WriteLine("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 « De : ». Cette adresse doit être vérifiée. Pour de plus amples informations, veuillez consulter [Identités vérifiées](#).
- Remplacez *recipient@example.com* par l'adresse « 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.
- *USWest2* Remplacez-le par le nom du Région AWS point de 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 Eclipse](#) créer 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 de ce didacticiel a été testé avec Eclipse Neon.3 (version 4.6.3), exécutant 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 pour 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 pour 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 pour Java)";
```

```
// The HTML body for the email.
static final String HTMLBODY = "<h1>Amazon SES test (AWS SDK pour 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 pour 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 pour PHP](#) pour envoyer un e-mail via Amazon SES.

Avant de commencer, exécutez les tâches suivantes :

- Installer PHP —PHP est disponible sur <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 pour PHP version 3 —Pour les instructions de téléchargement et d'installation, consultez la [AWS SDK pour 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 pour 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 pour 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 pour 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 pour PHP dans le programme. Pour en savoir plus, consultez la [documentation AWS SDK pour 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 pour 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) téléchargée, 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 pour Ruby](#) pour envoyer un e-mail via Amazon SES.

Avant de commencer, exécutez les tâches suivantes :

- Installer Ruby —Ruby est disponible sur. <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 pour Ruby —Pour obtenir des instructions de téléchargement et d'installation, consultez la section [Installation du AWS SDK pour Ruby](#) dans le guide du AWS SDK pour Ruby développeur. L'exemple de code inclus dans ce didacticiel a été testé avec la version 2.9.36 du kit AWS SDK pour 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 de plus amples informations, veuillez consulter [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 Kit SDK](#).

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

# The HTML body of the email.
htmlbody =
  '<h1>Amazon SES test (AWS SDK pour 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 pour Ruby</a>.'
```

```
# The email body for recipients with non-HTML email clients.
textbody = "This email was sent with Amazon SES using the AWS SDK pour 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 pour 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 de plus amples informations, veuillez consulter [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 pour Python (Boto) —Pour les instructions de téléchargement et d'installation, consultez la [AWS SDK pour 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 pour 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 pour 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 Kit 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

Si vous utilisez...	Enregistrez le fichier sous le nom...
Linux, macOS ou Unix	<code>~/.aws/credentials</code>

 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 Accept-Encoding d'en-tête 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 pour établir une TLS-encrypted connexion : 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

Bien que TLS 1.3 soit notre méthode de livraison par défaut, SES peut envoyer des e-mails aux serveurs de messagerie utilisant des versions antérieures de TLS.

Par défaut, Amazon SES utilise la méthode TLS opportuniste. Dans SES, le protocole TLS opportuniste utilise toujours STARTTLS et n'inclut pas le TLS Wrapper. Le flux implique l'établissement d'une connexion initiale en texte brut, suivie d'une mise à niveau vers une TLS-encrypted session si le client et le serveur prennent en charge STARTTLS. Si SES ne parvient pas à établir une connexion sécurisée, il envoie le message non chiffré.

Vous pouvez modifier ce comportement en utilisant des jeux de configurations. Utilisez l'opération [PutConfigurationSetDeliveryOptions](#) API 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 jeu 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.

End-to-end chiffrement

Vous pouvez utiliser Amazon SES pour envoyer des messages chiffrés à l'aide S/MIME de 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 S/MIME chiffrés :

- `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 PGP-encrypted e-mails :

- 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'opération `SendEmail` Amazon SES API v2 avec du contenu simple ou modélisé, ou si vous utilisez l'opération `SendBulkEmail`, 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

Utilisation des pièces jointes aux e-mails dans SES

Les pièces jointes aux e-mails dans SES sont des fichiers que vous pouvez inclure dans vos e-mails lorsque vous utilisez l'API SES v2 `SendEmail` et ses `SendBulkEmail` opérations. Cette fonctionnalité vous permet d'enrichir le contenu de vos e-mails en incluant des documents tels que des PDF, des fichiers Word, des images ou d'autres types de fichiers conformes aux types MIME pris en charge par SES. Vous pouvez également inclure des images intégrées qui s'affichent directement dans le contenu de l'e-mail sans que les destinataires n'aient à les télécharger séparément. Vous pouvez inclure plusieurs pièces jointes par e-mail, jusqu'à la limite de taille totale des messages de 40 Mo.

Note

[SendEmail](#) L'API SES v2 avec le type de Raw contenu, l'interface SMTP et l'API SES v1 continuent de gérer les pièces jointes par le biais de la construction de [messages MIME de courrier électronique bruts](#).

Comment fonctionnent les pièces jointes dans SES

Il existe deux types d'encodage différents qui se produisent à différents stades lors de l'envoi d'un e-mail avec pièces jointes :

Étape 1 — Envoi de données à SES :

- Lorsque vous souhaitez envoyer une pièce jointe à SES, les données binaires (comme un PDF ou une image) doivent être converties dans un format pouvant être transmis en toute sécurité.
- C'est là qu'intervient le codage base64 : il est obligatoire car vous ne pouvez pas envoyer de données binaires brutes dans une requête JSON.
- Si vous utilisez le AWS SDK, il gère automatiquement cet encodage.
- Si vous utilisez le AWS CLI, vous devez encoder vous-même la pièce jointe en base64 avant de l'envoyer.

Étape 2 — Création de l'e-mail par SES :

- Une fois que SES reçoit vos données, il doit créer un véritable e-mail avec la pièce jointe.
- C'est là que le [ContentTransferEncoding](#) décor entre en jeu.
- SES utilisera la méthode de codage que vous spécifiez ContentTransferEncoding pour formater automatiquement la pièce jointe dans l'e-mail final.

Pensez-y comme ceci : c'est comme envoyer un colis par la poste. Tout d'abord, vous devez faire parvenir le colis au bureau de poste (étape 1 - Base64-encoding obligatoire), puis le bureau de poste l'emballera de manière appropriée pour la livraison finale (étape 2 - ContentTransferEncoding).

Structure de l'objet de fixation

Lorsque vous envoyez un e-mail avec des pièces jointes via SES, le service gère automatiquement la construction complexe des messages MIME. Il vous suffit de fournir le contenu et les métadonnées de la pièce jointe via la structure d'[Attachment](#) objets suivante de l'API SES v2 :

- **FileName(Obligatoire)** — Le nom du fichier est affiché aux destinataires (doit inclure l'extension du fichier). S'il n'est pas fourni, SES Content Type dérivera un de l'extension du FileName.
- **ContentType(Facultatif)** : [identifiant du type de IANA-compliant média](#).
- **ContentDisposition(Facultatif)** — Spécifie le mode de rendu de la pièce jointe : ATTACHMENT (par défaut) ou INLINE.
- **ContentDescription(Facultatif)** — Brève description du contenu.
- **RawContent(Obligatoire)** — Le contenu réel de la pièce jointe.
- **ContentTransferEncoding(Facultatif)** — Spécifie la manière dont la charge utile de la pièce jointe est codée lorsqu'elle est assemblée dans le message MIME de l'e-mail : SEVEN_BIT (par défaut), BASE64 ou. QUOTED_PRINTABLE

Tout le contenu joint doit être encodé en base64 avant d'être transféré vers le point de terminaison SES pour envoi. Si vous utilisez le client AWS SDK pour effectuer des appels d'API, cela est automatiquement géré pour vous. Si vous utilisez ou avez implémenté votre propre client, vous devrez effectuer le codage vous-même, par exemple :AWS CLI

- Contenu en texte brut : Text attachment sample content.
- Encodé en Base64 : VGV4dCBhdHRhY2htZW50IHNhbnRlcjB250ZW50Lg==

Les exemples suivants montrent comment utiliser la structure d'objet de pièce jointe lors de la spécification de pièces jointes avec l'API SES v2 [SendEmail](#) et d'[SendBulkEmail](#) opérations utilisant le AWS CLI référencement d'un fichier JSON contenant des éléments d'objet de pièce jointe.

Exemple— SendEmail avec un contenu simple

```
aws sesv2 send-email --cli-input-json file://request-send-email-simple.json
```

request-send-email-simple.json

```
{
  "FromEmailAddress": "sender@example.com",
  "Destination": {
    "ToAddresses": [
      "recipient@example.com"
    ]
  },
  "Content": {
    "Simple": {
      "Subject": {
        "Data": "Email with attachment"
      },
      "Body": {
        "Text": {
          "Data": "Please see attached document."
        },
        "Html": {
          "Data": "Please see attached <b>document</b>."
        }
      }
    },
    "Attachments": [
      {
        "RawContent": "<base64-encoded-content>",
        "ContentDisposition": "ATTACHMENT",
        "FileName": "document.pdf",
        "ContentDescription": "PDF Document Attachment",
        "ContentTransferEncoding": "BASE64"
      }
    ]
  }
}
```

Exemple— SendEmail avec un contenu simple et une pièce jointe en ligne

```
aws sesv2 send-email --cli-input-json file://request-send-email-simple-inline-attachment.json
```

request-send-email-simple-inline-attachment.json

```
{
  "FromEmailAddress": "sender@example.com",
  "Destination": {
    "ToAddresses": [
      "recipient@example.com"
    ]
  },
  "Content": {
    "Simple": {
      "Subject": {
        "Data": "Email with attachment"
      },
      "Body": {
        "Html": {
          "Data": "<html><body>Our logo:<br><img src=\"cid:logo123\" alt=\\\"Company Logo\\\"></body></html>"
        }
      },
      "Attachments": [
        {
          "RawContent": "<base64-encoded-content>",
          "ContentDisposition": "INLINE",
          "FileName": "logo.png",
          "ContentId": "logo123",
          "ContentTransferEncoding": "BASE64"
        }
      ]
    }
  }
}
```

Exemple— SendEmail avec le contenu du modèle

```
aws sesv2 send-email --cli-input-json file://request-send-email-template.json
```

template-email-request-send-email.json

```
{
  "FromEmailAddress": "sender@example.com",
  "Destination": {
    "ToAddresses": [
      "recipient@example.com"
    ]
  },
  "Content": {
    "Template": {
      "TemplateName": "MyTemplate",
      "TemplateData": "{\"name\":\"John\"}",
      "Attachments": [
        {
          "RawContent": "<base64-encoded-content>",
          "ContentDisposition": "ATTACHMENT",
          "FileName": "document.pdf",
          "ContentDescription": "PDF Document Attachment",
          "ContentTransferEncoding": "BASE64"
        }
      ]
    }
  }
}
```

Example— SendBulkEmail avec contenu en pièce jointe

```
aws sesv2 send-bulk-email --cli-input-json file://request-send-bulk-email.json
```

request-send-bulk-email.json

```
{
  "FromEmailAddress": "sender@example.com",
  "DefaultContent": {
    "Template": {
      "TemplateName": "MyTemplate",
      "TemplateData": "{}",
      "Attachments": [
        {
          "RawContent": "<base64-encoded-content>",
          "ContentDisposition": "ATTACHMENT",

```

```
        "FileName": "document.pdf",
        "ContentDescription": "PDF Document Attachment",
        "ContentTransferEncoding": "BASE64"
    }
]
},
"BulkEmailEntries": [
    {
        "Destination": {
            "ToAddresses": [
                "recipient@example.com"
            ]
        },
        "ReplacementEmailContent": {
            "ReplacementTemplate": {
                "ReplacementTemplateData": "{\"name\":\"John\"}"
            }
        }
    }
]
```

Bonnes pratiques

- Limitez la taille totale des messages (pièces jointes comprises) à moins de 40 Mo.
- Dans la mesure du possible, laissez SES détecter automatiquement les types de contenu en fonction des extensions de fichiers.
- Spécifiez explicitement les types de contenu uniquement lorsqu'ils ne correspondent pas aux [types MIME courants](#).
- Envisagez d'utiliser des images intégrées pour un meilleur rendu des e-mails.
- SES prend en charge un large éventail de types MIME pour les pièces jointes, à l'exception de ceux répertoriés dans [Types de pièces jointes non pris en charge](#).

Types de pièces jointes SES non pris en charge

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 des traitements avancés, tels que livrer le courrier entrant dans un compartiment Amazon S3, le publier sur une rubrique Amazon SNS, l'envoyer à Amazon WorkMail ou envoyer automatiquement des messages de rebond lorsque les messages sont adressés 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 un Région AWS endroit où SES prend en charge la réception d'e-mails. Le tableau des [points de terminaison de réception d'e-mails](#) qui figure dans le tableau Références générales AWS répertorie tous ceux pour Régions AWS lesquels SES prend en charge la réception d'e-mails.

Rubriques de cette section :

- [Concepts de réception d'e-mails et cas d'utilisation Amazon SES](#)
- [Configuration de la réception d'e-mails via Amazon SES](#)
- [Instructions pour la console de réception d'e-mails Amazon SES](#)
- [Affichage des métriques pour la réception d'e-mails via Amazon SES](#)

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 niveau de IP-based contrôle étendu pour bloquer ou autoriser le courrier 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 :

- [Recipient-based contrôle à l'aide des règles de réception](#)
- [IP-based contrôle à l'aide de filtres d'adresses IP](#)
- [Email-receiving processus](#)
- [Cas d'utilisation et restrictions pour la réception d'e-mails Amazon SES](#)
- [Email-receiving authentification et analyse des logiciels malveillants](#)

Recipient-based contrôle à l'aide des 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 :

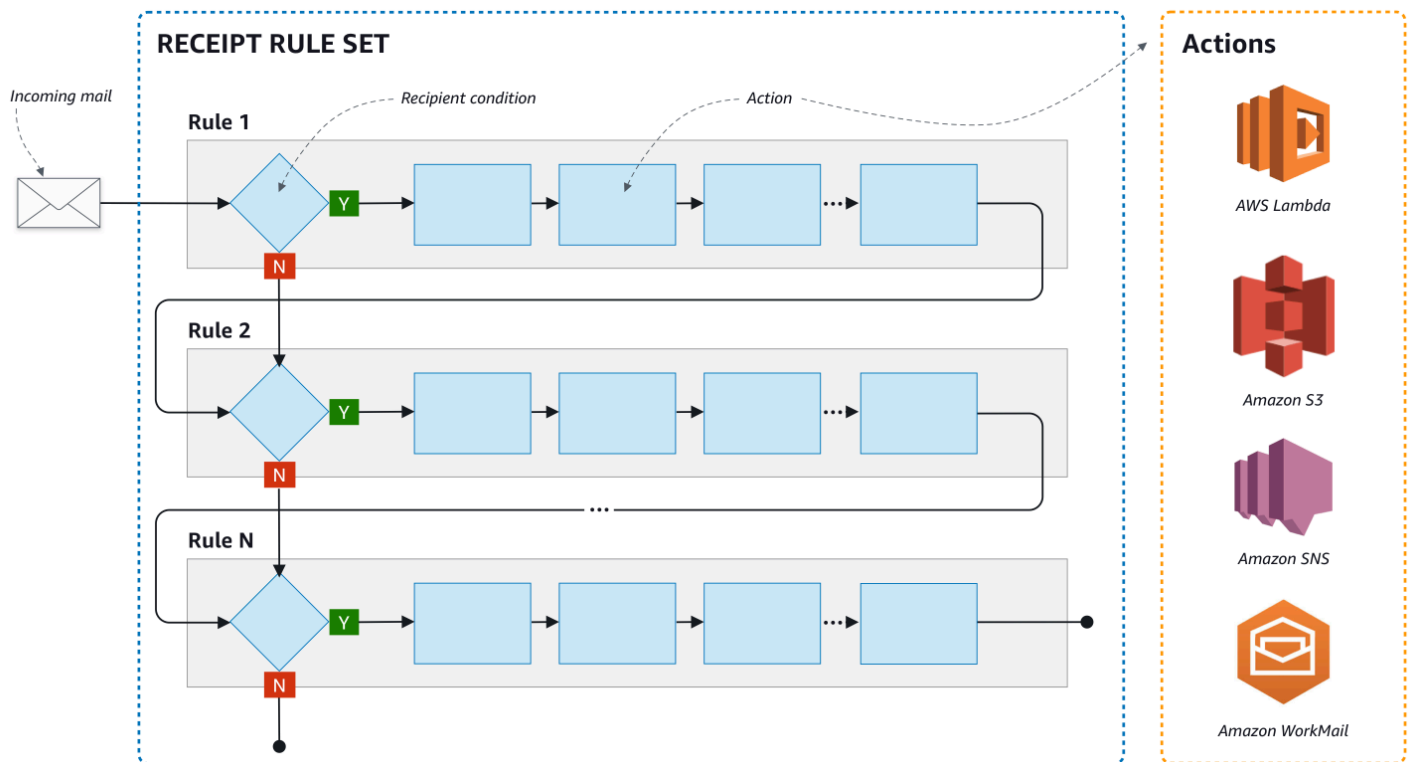
- Action Add header (Ajout d'en-tête) – Ajoute un en-tête à l'e-mail reçu. Vous utilisez généralement cette action uniquement en combinaison avec d'autres actions.
- Return bounce response action (Action de réponse de retour à l'expéditeur) : bloque l'e-mail en renvoyant une réponse de retour à l'expéditeur et vous avertit éventuellement via Amazon SNS.
- Invoquer une action de AWS Lambda fonction : appelle votre code via une fonction Lambda et, éventuellement, vous en informe 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.
- WorkMail Action d'intégration à Amazon : gère le courrier avec Amazon WorkMail. Vous n'utiliserez généralement pas cette action directement car Amazon WorkMail s'occupe 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 AWS compte, mais un seul ensemble de règles est actif à la fois. La figure suivante illustre les relations entre les règles, les ensembles de règles de réception et les actions.



IP-based contrôle 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](https://www.spamhaus.org/), 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.

Email-receiving processus

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 AWS régions. 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 avez besoin d'une solution capable à la fois d'envoyer et de recevoir des e-mails à l'aide d'un client de messagerie, pensez à utiliser [Amazon WorkMail](#).

En utilisant d'autres AWS services

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 donner accès à Amazon SES, vous devez créer des politiques relatives aux ressources à partir des consoles ou des API pour ces AWS services. 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 souhaitez 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 plus d'informations à ce sujet AWS Lambda, consultez le [guide du AWS Lambda développeur](#).

- 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) pour chiffrer éventuellement le courrier 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 pour Java](#) et le kit [AWS SDK pour 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 l'utiliser pour AWS Lambda envoyer des notifications de

rebond uniquement lorsque les messages échouent à l'authentification DKIM ou sont identifiés comme du spam. 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](#).

Email-receiving authentication et analyse des 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=permererror 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 pour détecter la présence de logiciels malveillants en fonction de la valeur de l'attribut ScanEnabled(API) ou de l'attribut d'analyse du spam et des virus (console) de la règle de réception correspondant à l'e-mail. Par défaut, SES recherche les logiciels malveillants dans le contenu des e-mails. Pour désactiver l'analyse du contenu des e-mails reçus qui correspondent à une règle de réception spécifique, vous devez définir l'ScanEnabledindicateur de la règle de réception sur False si vous [utilisez l'API](#), ou décocher la case Analyse du courrier indésirable et des 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.
- Donnez à Amazon SES l'autorisation d'accéder à d'autres AWS ressources afin d'exécuter des actions relatives aux règles 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. Il est nécessaire d'accorder des autorisations, car les actions que vous choisissez dans vos règles de réception ne fonctionneront que si Amazon SES est autorisé à utiliser le AWS service correspondant 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 éventuellement utiliser le SES [VerifyDomainDkim](#) ou [VerifyDomainIdentity](#) APIs.

Vous pouvez facilement confirmer que votre domaine ou adresse e-mail est vérifié en consultant son statut dans le tableau [des identités vérifiées](#) de la console SES ou en utilisant le SES [GetIdentityVerificationAttributes](#) ou [GetEmailIdentity](#) APIs.

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. L'enregistrement MX que vous créez fait référence au point de terminaison qui reçoit les e-mails de la AWS région 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 terminaux SES](#).

Note

Les points de terminaison qui reçoivent des e-mails dans Amazon SES ne sont ni des serveurs IMAP ni des serveurs de POP3 messagerie. Vous ne pouvez pas les utiliser URLs comme serveurs de courrier entrant dans les clients de messagerie. Si vous avez besoin d'une solution capable à la fois d'envoyer et de 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 enregistrement MX dépendent de votre DNS ou de votre fournisseur 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 ajouter un registre MX à la configuration DNS de votre domaine

1. (Prérequis) Pour effectuer ces procédures, vous devez modifier les enregistrements DNS de votre domaine. Si vous ne parvenez pas à accéder aux enregistrements DNS ou si cela ne vous convient pas, contactez votre administrateur système pour obtenir de l'aide.
2. Connectez-vous à la console de gestion de votre fournisseur DNS.
3. Créer un registre MX
4. 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

En fonction de votre fournisseur DNS : 1) La . fin de l'extension de domaine peut ne pas être requise. 2) Le champ Nom peut être appelé hôte, domaine ou domaine de messagerie.

5. Pour Type, choisissez MX.

Note

Certains fournisseurs DNS font référence au champ Type en tant que Type d' registre ou nom similaire.

6. 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 pour la AWS région 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 terminaux 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).

 Important

Les procédures spécifiques de création d'un registre MX dépendent de votre fournisseur DNS ou d'hébergement. Consultez la documentation de votre fournisseur ou contactez-le pour obtenir des informations sur l'ajout d'un enregistrement MX à la configuration DNS de votre domaine.

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)

Nom du fournisseur DNS/d'hébergement	Lien vers la documentation
HostGator	Modification des registres MX - Windows (lien externe)
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 SES, telles que l'envoi d'e-mails vers un bucket Amazon Simple Storage Service (Amazon S3) ou l'appel d' AWS Lambda une fonction, nécessitent des autorisations spéciales. Cette section inclut des exemples de stratégies pour plusieurs cas d'utilisation courants.

Rubriques de cette section :

- [Configuration des autorisations de rôle IAM pour l'action de compartiment Deliver to S3](#)
- [Autoriser SES à écrire dans un compartiment S3](#)
- [Autorisez SES à utiliser votre AWS KMS clé](#)
- [Autoriser SES à invoquer une AWS Lambda fonction](#)
- [Autoriser SES à publier sur une rubrique Amazon SNS appartenant à un autre compte AWS](#)

Configuration des autorisations de rôle IAM pour l'action de compartiment Deliver to S3

Les points suivants s'appliquent à ce rôle IAM :

- Il ne peut être utilisé que pour [Livrer à l'action du compartiment S3](#).
- Il doit être utilisé si vous souhaitez écrire dans un compartiment S3 qui existe dans une région où SES [the section called “Réception d'e-mails”](#) n'est pas disponible.

Si vous souhaitez écrire dans un compartiment S3, vous pouvez fournir un rôle IAM avec des autorisations permettant d'accéder aux ressources pertinentes pour le [Livrer à l'action du compartiment S3](#). Vous devez également autoriser SES à assumer ce rôle pour effectuer l'action par le biais d'une politique de confiance IAM, comme expliqué dans la [section suivante](#).

Cette politique d'autorisation doit être collée dans l'éditeur de politique en ligne du rôle IAM. Consultez [Livrer à l'action du compartiment S3](#) et suivez les étapes indiquées dans l'élément de rôle IAM. (L'exemple suivant inclut également des autorisations facultatives au cas où vous souhaiteriez utiliser la notification par sujet SNS ou une clé gérée par le client dans l'action S3.)

Note

- Vous avez la possibilité de configurer l'action S3 sans spécifier de rôle IAM en autorisant uniquement le service SES dans la politique du compartiment S3, comme indiqué [the section called "Autoriser SES à écrire dans un compartiment S3"](#). Cela fonctionnera également pour les scénarios entre comptes.
- Si vous spécifiez un rôle IAM pour l'action S3, SES assume ce rôle pour l'opération « PutObject », et les autorisations IAM spécifiées ici seront suffisantes pour une utilisation identique du compte. Toutefois, pour une utilisation entre comptes, vous aurez besoin d'une politique de compartiment supplémentaire qui autorise le rôle IAM à « PutObject » figurer dans le compartiment. Ceci est spécifié par le propriétaire du compartiment qui accorde des autorisations de compartiment entre comptes, comme expliqué dans la section [Le propriétaire du compartiment accorde des autorisations de compartiment entre comptes](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3Access",
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    {
      "Sid": "SNSAccess",
```



```
        "Effect": "Allow",
        "Action": "sns:Publish",
        "Resource": "arn:aws:sns:us-east-1:111122223333:my-topic"
    },
    {
        "Sid": "KMSAccess",
        "Effect": "Allow",
        "Action": "kms:GenerateDataKey*",
        "Resource": "arn:aws:kms:us-east-1:111122223333:key/key-id"
    }
  ]
}
```

Dans l'exemple précédent, apportez les modifications suivantes :

- *amzn-s3-demo-bucket* Remplacez-le par le nom du compartiment S3 dans lequel vous souhaitez écrire.
- Remplacez *region* par l' Région AWS endroit où vous avez créé la règle de réception.
- Remplacez *111122223333* par votre ID de compte AWS .
- *my-topic* Remplacez-le par le nom de la rubrique SNS pour laquelle vous souhaitez publier des notifications.
- *key-id* Remplacez-le par l'ID de votre clé KMS.

Politique de confiance pour le rôle IAM d'action S3

La politique de confiance suivante doit être ajoutée aux relations de confiance du rôle IAM pour permettre à SES d'assumer ce rôle.

Note

L'ajout manuel de cette politique de confiance n'est requis que si vous n'avez pas créé votre rôle IAM à partir de la console SES en suivant les étapes indiquées dans l'élément de rôle IAM du [Livrer à l'action du compartiment S3](#) flux de travail. Lorsque vous créez le rôle IAM depuis la console, cette politique de confiance est automatiquement générée et appliquée au rôle pour vous, ce qui rend cette étape inutile.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSESAssume",
      "Effect": "Allow",
      "Principal": {
        "Service": "ses.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "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 l' Région AWS endroit où vous avez créé la règle de réception.
- Remplacez *111122223333* par votre ID de compte AWS .
- Remplacez *rule_set_name* par le nom de l'ensemble de règles qui contient la règle de réception contenant l'action de livraison vers le compartiment Amazon S3.
- *receipt_rule_name* Remplacez-le par le nom de la règle de réception qui contient l'action de livraison vers le compartiment Amazon S3.

Autoriser SES à écrire dans un compartiment S3

Lorsque vous appliquez la politique suivante à un compartiment S3, cela donne à SES l'autorisation d'écrire dans ce compartiment tant qu'il existe dans une région où la [réception d'e-mails](#) SES est disponible. Si vous souhaitez écrire dans un compartiment situé en dehors d'une région de réception d'e-mails, consultez. [Configuration des autorisations de rôle IAM pour l'action de compartiment](#)

[Deliver to S3](#) 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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSESPuts",
      "Effect": "Allow",
      "Principal": {
        "Service": "ses.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "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 :

- *amzn-s3-demo-bucket* Remplacez-le par le nom du compartiment S3 dans lequel vous souhaitez écrire.
- Remplacez *region* par la AWS région dans laquelle vous avez créé la règle de réception.
- Remplacez *111122223333* par votre ID de compte AWS .
- Remplacez *rule_set_name* par le nom de l'ensemble de règles qui contient la règle de réception contenant l'action de livraison vers le compartiment Amazon S3.

- ***receipt_rule_name*** Remplacez-le par le nom de la règle de réception qui contient l'action de livraison vers le compartiment Amazon S3.

Autorisez SES à utiliser votre AWS KMS clé

Pour que SES puisse chiffrer vos e-mails, il doit être autorisé à utiliser la AWS KMS clé que vous avez spécifiée lors de la configuration de 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 d'étapes supplémentaires pour autoriser SES à l'utiliser. Si vous utilisez une clé gérée par le client, vous devez autoriser SES à l'utiliser en ajoutant une déclaration à la politique de la clé.

Utilisez la déclaration de politique suivante comme politique clé pour autoriser SES à utiliser votre clé gérée par le client lorsqu'elle 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 AWS région dans laquelle vous avez créé la règle de réception.
- Remplacez ***111122223333*** par votre ID de compte AWS .
- Remplacez ***rule_set_name*** par le nom de l'ensemble de règles contenant la règle de réception que vous avez associée à la réception d'e-mails.

- ***receipt_rule_name*** Remplacez-le par le nom de la règle de réception que vous avez associée à la réception d'e-mails.

Si vous avez l'habitude AWS KMS d'envoyer des messages chiffrés à un compartiment S3 avec le chiffrement côté serveur activé, vous devez ajouter l'action de politique, "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 plus d'informations sur l'association de politiques aux AWS KMS clés, consultez la section [Utilisation des politiques clés AWS KMS dans](#) le manuel du AWS Key Management Service développeur.

Autoriser SES à invoquer une AWS Lambda fonction

Pour permettre à SES d'appeler une AWS Lambda fonction, vous pouvez choisir la fonction lorsque vous créez une règle de réception dans la console SES. Lorsque vous le faites, 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 suivant à l'`AddPermission` API autorise 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 AWS région dans laquelle vous avez créé la règle de réception.
- Remplacez *111122223333* par votre ID de compte AWS .
- Remplacez *rule_set_name* par le nom de l'ensemble de règles contenant 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.

Autoriser SES à publier sur une rubrique Amazon SNS appartenant à un autre compte AWS

Pour publier des notifications relatives à un sujet dans un AWS compte distinct, vous devez associer une politique au sujet Amazon SNS. La rubrique SNS doit se trouver dans la même région que le jeu de règles de réception et de domaine.

La politique suivante autorise SES à publier sur une rubrique Amazon SNS dans un compte distinct AWS .

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ses.amazonaws.com"
      },
      "Action": "SNS:Publish",
```

```

        "Resource": "arn:aws:sns:us-east-1:111122223333:topic_name",
        "Condition": {
            "StringEquals": {
                "AWS:SourceAccount": "444455556666",
                "AWS:SourceArn": "arn:aws:ses:us-east-1:777788889999:receipt-
rule-set/rule_set_name:receipt-rule/rule_name"
            }
        }
    }
]
}

```

Dans l'exemple précédent, apportez les modifications suivantes :

- *topic_region* Remplacez-le par Région AWS celui dans lequel le sujet Amazon SNS a été créé.
- *sns_topic_account_id* Remplacez-le par l'ID du AWS compte propriétaire de la rubrique Amazon SNS.
- *topic_name* Remplacez-le par le nom de la rubrique Amazon SNS pour laquelle vous souhaitez publier des notifications.
- Remplacez *aws_account_id* par l'ID du AWS compte configuré pour recevoir des e-mails.
- Remplacez *receipt_region* par l' Région AWS endroit où vous avez créé la règle de réception.
- *rule_set_name* Remplacez-le par le nom de l'ensemble de règles contenant la règle de réception dans laquelle vous avez créé votre action de rubrique de publication sur Amazon SNS.
- *receipt_rule_name* Remplacez-le par le nom de la règle de réception contenant l'action de rubrique de publication sur Amazon SNS.

Si votre rubrique Amazon SNS utilise AWS KMS le chiffrement côté serveur, vous devez ajouter des autorisations à la politique clé. AWS KMS Vous pouvez ajouter des autorisations en joignant la politique suivante à la politique AWS KMS clé :

JSON

```

{
    "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 rendue dépendante de la première condition du destinataire ; si elle n'est pas spécifiée, les actions seront appliquées à toutes les identités appartenant 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.

Conditions préalables

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 terminal se trouve dans un Région AWS endroit où Amazon SES prend en charge la réception d'e-mails. Le tableau des [points de terminaison de réception d'e-mails](#) qui figure dans le tableau Références générales AWS répertorie les points de terminaison de réception d'e-mails pour tous ceux Régions AWS où SES prend en charge la réception d'e-mails.
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. (L'enregistrement MX doit faire référence au point de terminaison Amazon SES qui reçoit le courrier pour la AWS région dans laquelle vous utilisez Amazon SES.)
4. Enfin, vous devez [autoriser Amazon SES](#) à accéder à d'autres AWS ressources afin d'exécuter les actions relatives aux règles 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 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 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 “Conditions préalables”](#).

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 correspondance une adresse e-mail spécifique.	utilisateur@exemple.com	Met également en correspondance les variations de l'adresse qui contiennent des étiquettes (par exemple, utilisateur+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.	exemple.com	
Mettre en correspondance les adresses au sein d'un sous-domaine spécifique	subdomain.exemple.com	

Si vous souhaitez...	Spécifier les destinataires suivants...	Remarques
e, mais pas celles dans le domaine parent.		
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.

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 AWS Lambda.
 - [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.
 - [Intégrer à Amazon WorkMail](#) - Cette action 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 répertoriées dans le tableau Actions de la page de révision en utilisant les up/down flèches de la colonne 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](#)
- [Intégrer à Amazon WorkMail Action](#)

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.

 Note

Les messages Bounce ne sont pas envoyés via votre domaine MAIL FROM personnalisé, mais sont générés en interne par SES et signés uniquement avec la signature amazonses.com DKIM. Pour contourner le problème, utilisez l'option Expéditeur de réponse pour définir une adresse e-mail pour vos messages de rebond. Consultez cet [AWS re:Post article](#) pour plus d'informations.

- 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 se trouver dans la même AWS région 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'invocation `RequestResponse` signifie 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.

Exigences

- La fonction Lambda que vous choisissez doit se trouver dans la même AWS région que le point de terminaison Amazon SES que vous utilisez pour recevoir des e-mails.
- La rubrique Amazon SNS que vous choisissez doit se trouver dans la même AWS région 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 des exemples de AWS Lambda code, voir [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 présentent des exemples d'événements liés au courrier entrant, des exemples de cas d'utilisation de haut niveau et des exemples de AWS Lambda code :

- [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 à 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 de l'événement dans un journal. CloudWatch Les exemples de fonctions Lambda dans [Exemples de fonctions Lambda](#) log to. 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.

```
export const handler = async (event, context, callback) => {
  console.log('Spam filter');

  const 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, {'disposition':'CONTINUE'});
  }
};
```

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.

```
export const handler = async (event, context, callback) => {
  console.log('Header matcher');

  const sesNotification = event.Records[0].ses;
  console.log("SES Notification:\n", JSON.stringify(sesNotification, null, 2));

  // Iterate over the headers
  for (let index in sesNotification.mail.headers) {
    const 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, {'disposition':'CONTINUE'});
      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.
- [Assurez-vous que la fonction Lambda dispose des autorisations IAM pour récupérer des objets depuis le compartiment S3. Reportez-vous à cet article de Re:Post pour plus d'informations.AWS](#)
- Il est possible que les délais d'exécution Lambda par défaut soient trop courts pour votre flux de travail. Pensez à les augmenter.

```
import { S3Client, GetObjectCommand } from "@aws-sdk/client-s3";
const bucketName = '<Your Bucket Name>';

export const handler = async (event, context, callback) => {
  const client = new S3Client();
  console.log('Process email');

  var sesNotification = event.Records[0].ses;
  console.log("SES Notification:\n", JSON.stringify(sesNotification, null, 2));
  console.log("MessageId: " + sesNotification.mail.messageId)

  const getObjectCommand = new GetObjectCommand({
    Bucket: bucketName,
    Key: sesNotification.mail.messageId
  });

  try {
    const response = await client.send(getObjectCommand);
    const receivedMail = await response.Body.transformToString();
    console.log(receivedMail);
    callback(null, {'disposition':'CONTINUE'})
  } catch (e) {
```

```
// Perform error handling here
console.log("Encountered S3 client error: "+ e, e.stack);
callback(null, {'disposition':'STOP_RULE_SET'})
}
};
```

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.
- Assurez-vous que la fonction Lambda dispose des `ses:SendBounce` autorisations nécessaires pour l'identité SES qui envoie les messages de rebond.

```
import { SESClient, SendBounceCommand } from "@aws-sdk/client-ses";
const sesClient = new SESClient();
// Assign the emailDomain environment variable to a constant.
const emailDomain = process.env.emailDomain;

export const handler = async (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));

    const sendBounceCommand = new SendBounceCommand(sendBounceParams);

    // Try to send the bounce.
    try {
        const response = await sesClient.send(sendBounceCommand);
        console.log(response);
        console.log(`Bounce for message ${messageId} sent, bounce message ID:
${response.MessageId}`);
        // Stop processing additional receipt rules in the rule set.
        callback(null, {disposition: 'STOP_RULE_SET'});
    } catch (e) {
        // If something goes wrong, log the issue.
        console.log(`An error occurred while sending bounce for message:
${messageId}`, e);
        // Perform any additional error handling here
        callback(e)
    }

    // 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(null, {disposition: 'CONTINUE'});
    }
};

```

Livrer à l'action du compartiment S3

L'action Livrer au compartiment S3 envoie le courrier à un compartiment S3 et peut éventuellement vous avertir via SNS et plus encore. Cette action comporte les options suivantes.

- **Compartiment S3** : nom du compartiment S3 dans lequel enregistrer les e-mails reçus. Vous pouvez également créer un nouveau compartiment S3 lorsque vous configurez votre action en choisissant Create S3 Bucket. 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

- Le compartiment Amazon S3 doit exister dans une région où SES [the section called “Réception d'e-mails”](#) est disponible ; sinon, vous devez utiliser l'option de rôle IAM expliquée ci-dessous.
 - Lorsque vous enregistrez vos e-mails dans un compartiment S3, la taille maximale par défaut (en-têtes compris) est de 40 Mo.
 - 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, veuillez 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](#).
- **Préfixe de clé d'objet** : préfixe de nom de clé facultatif à utiliser dans le compartiment S3. Les préfixes de nom de clé vous permettent d'organiser votre compartiment S3 dans une structure de dossiers. Par exemple, si vous utilisez Email comme préfixe de clé d'objet, vos e-mails apparaîtront dans votre compartiment S3 dans un dossier nommé Email.
 - **Chiffrement des messages** : option permettant de chiffrer les e-mails reçus avant de les envoyer dans votre compartiment S3.
 - **Clé de chiffrement KMS** — (Disponible si le chiffrement des messages est sélectionné.) La AWS KMS clé que SES doit utiliser pour chiffrer vos e-mails avant de les enregistrer dans le compartiment S3. Vous pouvez utiliser la clé KMS par défaut ou une clé gérée par le client que vous avez créée dans KMS.

 Note

La clé KMS que vous choisissez doit se trouver dans la même AWS région que le point de terminaison 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 SES. Si vous utilisez l'API SES, vous pouvez spécifier la clé KMS par défaut en fournissant un ARN sous la forme `dearn:aws:kms:REGION:AWSACCOUNTID:alias/aws/ses`. Par exemple, si votre identifiant de AWS compte 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 serait `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 d'étapes supplémentaires pour autoriser SES à utiliser la clé.
- Pour utiliser une clé gérée par le client que vous avez créée dans KMS, fournissez l'ARN de la clé KMS et assurez-vous d'ajouter une déclaration à la politique de votre clé pour autoriser 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 plus d'informations sur l'utilisation de KMS avec SES, consultez le [manuel du AWS Key Management Service développeur](#). Si vous ne spécifiez pas de clé KMS dans la console ou dans l'API, SES ne chiffrera pas vos e-mails.

 Important

Votre courrier est crypté par SES à l'aide du client de chiffrement S3 avant qu'il ne soit envoyé à S3 pour stockage. Il n'est pas chiffré à l'aide du chiffrement S3 côté serveur. Cela signifie que vous devez utiliser le client de chiffrement S3 pour déchiffrer le courrier électronique après l'avoir récupéré auprès de S3, car le service n'a pas accès à vos clés KMS pour le déchiffrement. Ce client de chiffrement est disponible dans le kit [AWS SDK pour Java](#) et le kit [AWS SDK pour Ruby](#). Pour en savoir plus, veuillez consulter [Guide de l'utilisateur Amazon Simple Storage Service](#).

- Rôle IAM : rôle IAM utilisé par SES pour accéder aux ressources de l'action `Deliver to S3` (compartiment Amazon S3, rubrique SNS et clé KMS). Si ce n'est pas le cas, vous devrez

explicitement autoriser SES à accéder à chaque ressource individuellement [Attribution d'autorisations à Amazon SES pour la réception d'e-mails](#) (voir.

Si vous souhaitez écrire dans un compartiment S3 qui existe dans une région où la réception d'e-mails SES n'est pas disponible, vous devez utiliser un rôle IAM doté de la politique d'autorisation d'écriture dans S3 comme politique intégrée du rôle. Vous pouvez appliquer la politique d'autorisation pour cette action directement depuis la console :

1. Choisissez Créer un nouveau rôle dans le champ Rôle IAM et entrez un nom suivi de Créer un rôle. (La politique de confiance IAM pour ce rôle sera automatiquement générée en arrière-plan.)
 2. Comme la politique de confiance IAM a été générée automatiquement, il vous suffit d'ajouter la politique d'autorisation de l'action au rôle. Sélectionnez Afficher le rôle dans le champ Rôle IAM pour ouvrir la console IAM.
 3. Sous l'onglet Autorisations, choisissez Ajouter des autorisations, puis sélectionnez Créer une politique intégrée.
 4. Sur la page Spécifier les autorisations, sélectionnez JSON dans l'éditeur de politiques.
 5. Copiez et collez la politique d'autorisation depuis [Autorisations de rôle IAM pour l'action S3](#) l'éditeur de politique et remplacez les données en texte rouge par les vôtres. (Assurez-vous de supprimer tout exemple de code dans l'éditeur.)
 6. Choisissez Suivant.
 7. Passez en revue et créez votre politique d'autorisation pour le rôle IAM en choisissant Créer une politique.
 8. Sélectionnez l'onglet de votre navigateur où la page SES Create rule — Add actions est ouverte et poursuivez les étapes restantes pour créer des règles.
- Rubrique SNS : nom ou ARN de la rubrique Amazon SNS à avertir lorsqu'un e-mail est enregistré dans le compartiment S3. Voici un exemple d'ARN de rubrique SNS : `arn:aws:sns:us-east-1:123456789012 :. MyTopic` Vous pouvez également créer un sujet SNS lorsque vous configurez votre action en choisissant Créer un sujet SNS. Pour plus d'informations sur les sujets liés aux réseaux sociaux, consultez le [guide du développeur Amazon Simple Notification Service](#).

 Note

- La rubrique SNS que vous choisissez doit se trouver dans la même AWS région que le point de terminaison SES que vous utilisez pour recevoir des e-mails.

- N'utilisez le chiffrement des clés KMS géré par le client qu'avec les rubriques SNS que vous associez aux règles de réception de SES, car vous devrez modifier la politique des clés KMS pour autoriser SES à publier sur SNS. Cela contraste avec les politiques clés KMS AWS gérées qui ne peuvent pas être modifiées dès leur conception.

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 se trouver dans la même AWS région que le point de terminaison Amazon SES que vous utilisez pour recevoir des e-mails.
- N'utilisez le chiffrement des clés KMS géré par le client qu'avec les rubriques SNS que vous associez aux règles de réception de SES, car vous devrez modifier la politique des

clés KMS pour autoriser SES à publier sur SNS. Cela contraste avec les politiques clés KMS AWS gérées qui ne peuvent pas être modifiées dès leur conception.

- 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 depuis d'autres types d'actions : lorsque vous ajoutez un autre type d'action (notamment [Bounce](#), [Lambda](#), [Stop Rule Set](#) [WorkMail](#) ou actions) à une règle de réception, vous pouvez éventuellement spécifier une rubrique Amazon SNS. 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 relatives à la réception d'e-mails sont publiées dans les rubriques Amazon Simple Notification Service (Amazon SNS) JavaScript au format JSON (Object Notation).

Pour des exemples de notifications, consultez [Exemples de notification](#) .

Table des matières

- [Objet JSON de niveau supérieur](#)

- [Objet receipt](#)
 - [Objets action](#)
 - [Objet dkimVerdict](#)
 - [Objet dmarcVerdict](#)
 - [Objet spamVerdict](#)
 - [Objet spfVerdict](#)
 - [Objet virusVerdict](#)
- [Objet mail](#)
 - [Objet commonHeaders](#)

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 .  Note Ce champ est disponible uniquement si la notification a été déclenchée par une action SNS. Les notifications déclenché

Nom de champ	Description
	es par toutes les autres actions ne contiennent pas ce champ.

Objet receipt

L'objet receipt comporte les champs suivants.

Nom de champ	Description
<u>action</u>	Objet qui encapsule des informations sur l'action qui a été exécutée. Pour obtenir une liste des valeurs possibles, consultez <u>Objets action</u> .
<u>dkimVerdict</u>	Objet qui indique si le contrôle du courrier DomainKeys identifié (DKIM) a réussi. Pour obtenir une liste des valeurs possibles, consultez <u>Objet dkimVerdict</u> .
dmARCPolicy	Indique les paramètres DMARC (Domain-based 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 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

Nom de champ	Description
	soit traités comme étant suspects par les serveurs de messagerie. • <code>reject</code> : Le propriétaire du domaine d'envoi demande que les messages pour lesquels l'authentification DMARC échoue soient rejetés.
<code>dmarcVerdict</code>	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 .
<code>processingTimeMillis</code>	Chaîne qui spécifie le délai, en millisecondes, entre le moment où Amazon SES reçoit le message et le moment où l'action est déclenchée.
<code>recipients</code>	Une liste des destinataires (plus particulièrement les adresses RCPT TO de l'enveloppe) qui ont été retrouvés par la règle de réception active. Les adresses répertoriées ici peuvent être différentes de celles figurant dans le champ <code>destination</code> de l'objet the section called "Objet mail" .
<code>spamVerdict</code>	Objet qui indique si le message est un courrier indésirable. Pour obtenir une liste des valeurs possibles, consultez Objet spamVerdict .
<code>spfVerdict</code>	Objet qui indique si le contrôle SPF (Sender Policy Framework) a réussi. Pour obtenir une liste des valeurs possibles, consultez Objet spfVerdict .

Nom de champ	Description
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.
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.

Nom de champ	Description
<code>statusCode</code>	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.
<code>message</code>	Chaîne qui contient le texte lisible par l'utilisateur à inclure dans le message de retour à l'expéditeur. Présente uniquement pour le type de retour à l'expéditeur.
<code>sender</code>	Chaîne qui contient l'adresse e-mail de l'expéditeur 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'expéditeur.
<code>functionArn</code>	Chaîne qui contient l'ARN de la fonction Lambda qui a été déclenchée. Présente uniquement pour le type d'action Lambda.
<code>invocationType</code>	Chaîne qui contient le type d'appel de la fonction Lambda. Les valeurs possibles sont <code>RequestResponse</code> et <code>Event</code> . Présente uniquement pour le type d'action Lambda.
<code>organizationArn</code>	Chaîne contenant l'ARN de l'organisation Amazon WorkMail. Présent uniquement pour le type WorkMail d'action.

Objet dkimVerdict

L'objet dkimVerdict comporte les champs suivants.

Nom de champ	Description
<code>status</code>	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 correctement.

Objet `dmARCVerdict`

L'objet `dmARCVerdict` comporte les champs suivants.

Nom de champ	Description
<code>status</code>	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. • GRAY : au moins une authentification SPF ou DKIM a passé l'authentification, mais le domaine d'envoi ne dispose pas d'une

Nom de champ	Description
	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
<code>status</code>	Chaîne qui contient le résultat du contrôle SPF. Les valeurs possibles sont : • <code>PASS</code> : Authentification SPF réussie pour le message. • <code>FAIL</code> : Échec de l'authentification SPF pour le message. • <code>GRAY</code> : Le résultat SPF est <code>none</code>, <code>softfail</code> ou <code>neutral</code>. • <code>PROCESSING_FAILED</code> : 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
<code>status</code>	Chaîne qui contient le résultat de la recherche de virus. Les valeurs possibles sont : • <code>PASS</code> : Le message ne contient pas de virus. • <code>FAIL</code> : Le message contient un virus. • <code>GRAY</code> : Amazon SES a analysé l'e-mail mais n'a pas pu déterminer avec fiabilité s'il contient un virus. • <code>PROCESSING_FAILED</code> : Amazon SES n'est pas en mesure d'analyser le contenu de 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
<code>destination</code>	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.
<code>messageId</code>	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.
<code>source</code>	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.
<code>timestamp</code>	Chaîne contenant l'heure à laquelle l'e-mail a été reçu, au ISO8601 format.
<code>headers</code>	Les en-têtes Amazon SES et vos en-têtes personnalisés. Chaque en-tête possède les champs suivants : <code>name</code> et <code>value</code> .
<u><code>commonHeaders</code></u>	Les en-têtes communs à tous les e-mails. Chaque en-tête possède les champs suivants : <code>name</code> et <code>value</code> .
<code>headersTruncated</code>	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 <code>true</code> et <code>false</code> .

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
<code>messageId</code>	ID du message original.
<code>date</code>	Date et heure auxquelles Amazon SES a reçu le message.
<code>to</code>	L'en-tête To de l'e-mail.
<code>cc</code>	L'en-tête CC de l'e-mail.
<code>bcc</code>	L'en-tête BCC de l'e-mail.
<code>from</code>	L'en-tête From de l'e-mail.
<code>sender</code>	L'en-tête Sender de l'e-mail.
<code>returnPath</code>	L'en-tête Return-Path de l'e-mail.
<code>replyTo</code>	L'en-tête Reply-To de l'e-mail.
<code>subject</code>	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 :

- [Notification envoyée à la suite d'une action sur le réseau social.](#)
- [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-BEC9-87BCBF2211C9@example.com",
    "messageId": "d6iitobk75ur44p8kdnp7g2n800",
    "destination": [
      "recipient@example.com"
    ],
    "headersTruncated": false,
    "headers": [
      {
        "name": "Return-Path",

"value": "<0000014fbe1c09cf-7cb9f704-7531-4e53-89a1-5fa9744f5eb6-0000000@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
```

```

d6iitobk75ur44p8kdnp7g2n800 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=ug7nbt4gccmlpwj322ax3p6ow6yfsug; d=amazonses.com; t=1442003552;
h=From:To:Subject:MIME-Version:Content-Type:Content-Transfer-Encoding:Date:Message-
ID:Feedback-ID; bh=DWr3I0mYWoXCA9ARqGC/UaODfghffiwFNRIb2Mckyt4=;
b=p4ukUDSFqhqiub+zPR0DW1kp7oJZakrzupr6LBe6sUuvqpBkig56UzUwc29rFbJF
hlX30v7DeYVNoN38stqwsF8ivcajXpQsXRC1cW9z8x875J041rClAjV7EGbLmudVpPX
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/p0PpEPSHn2u2o4=: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 d6iitobk75ur44p8kdnp7g2n800\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\t s=ug7nbt4gccmlpwj322ax3p6ow6yfsug; d=amazonses.com; t=1442003552;\r\n\t h=From:To:Subject:MIME-Version:Content-Type:Content-Transfer-Encoding:Date:Message-ID:Feedback-ID;\r\n\t bh=DWr3IOmYWoXCA9ARqGC/Ua0DfghffiwFNRIb2Mckyt4=;\r\n\t b=p4ukUDSFqhqiub+zPR0DW1kp7oJZakrzupr6LBe6sUuvqpBkig56UzUwc29rFbJF\r\n\t h1X30v7DeYVNoN3stqwsF8ivcajXpQsXRC1cW9z8x875J041rClAjV7EGbLmudVpPX\r\n\t 4hHst1XPyX5wmgdHIhmUuh8oZKpVqGi6bHGzzf7g=\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/p0PpEPSHn2u2o4=: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": "0000014fbelc09cf-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
d6iitobk75ur44p8kdnp7g2n800 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=ug7nbt4gccmlpwj322ax3p6ow6yfsug; 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
h1X30v7DeYVNoN38stqwsF8ivcajXpQsXRC1cW9z8x875J041rClAjV7EGbLmudVpPX
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/p0PpEPSHn2u2o4=: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 se trouver dans la même AWS région que le point de terminaison Amazon SES que vous utilisez pour recevoir des e-mails.

Intégrer à Amazon WorkMail Action

L'WorkMailaction s'intègre à Amazon WorkMail. Si Amazon WorkMail effectue l'ensemble du traitement de vos e-mails, vous n'utiliserez généralement pas cette action directement, car Amazon WorkMail s'occupe de la configuration. Cette action comporte les options suivantes.

- ARN de l'organisation : ARN de l'organisation Amazon WorkMail. L'organisation Amazon ARNs se présente sous la forme `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'identifiant du AWS compte. Vous trouverez votre identifiant de AWS compte sur la page [Compte](#) de la console de AWS gestion.
 - `organization_ID` est un identifiant unique WorkMail généré par Amazon lorsque vous créez une organisation. Vous pouvez trouver l'identifiant de l'organisation dans la WorkMail console Amazon sur la page des paramètres de votre organisation.

Voici un exemple d'ARN complet d'une WorkMail organisation Amazon : `arn:aws:workmail:us-east-1:123456789012:organization/m-68755160c4cb4e29a2b2f8fb58f359d7`. Pour plus d'informations sur WorkMail les organisations Amazon, consultez le [guide de WorkMail l'administrateur Amazon](#).

- Rubrique SNS : nom ou ARN de la rubrique Amazon SNS à avertir lorsque l'action WorkMail Amazon est entreprise. 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 se trouver dans la même AWS région que le point de terminaison Amazon SES que vous utilisez pour recevoir des e-mails.

Note

Amazon SES ne prend en charge les WorkMail actions que dans les régions où WorkMail elles sont disponibles. Consultez les [WorkMail points de terminaison et les quotas Amazon](#) 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. (L'enregistrement MX doit faire référence au point de terminaison Amazon SES qui reçoit le courrier pour la AWS région dans laquelle 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 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 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

Scope	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
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

Scope	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

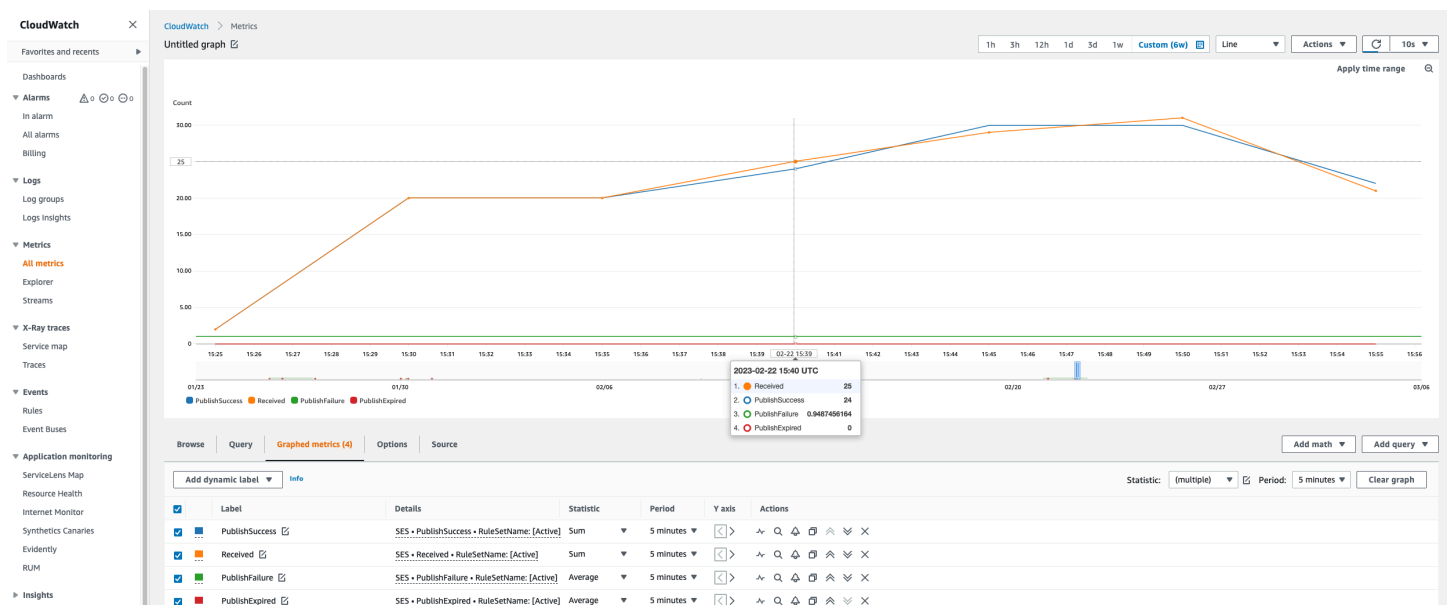
- Dans les tableaux précédents, le terme « s'applique » signifie que l'expéditeur n'est pas bloqué par les filtres IP ou qu'il figure dans la liste de blocage interne de SES, et que des conditions de destinataire et la politique TLS correspondent pour la règle.

- Des erreurs liées 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.

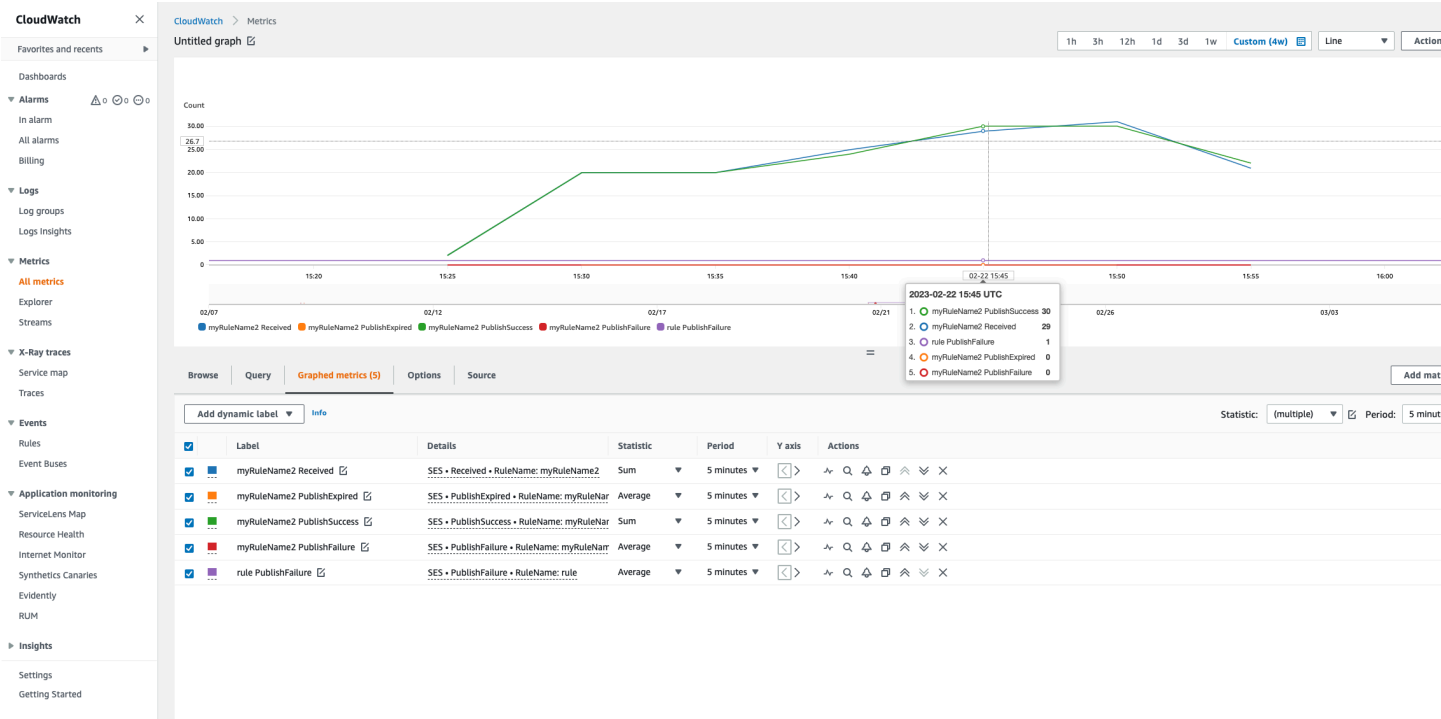
⚠ Important

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.



Locataires

Ce chapitre explique comment utiliser la gestion des locataires Amazon SES pour isoler, surveiller et gérer l'envoi d'e-mails entre plusieurs locataires au sein de votre compte SES. Cette fonctionnalité aide les fournisseurs de logiciels indépendants (ISV), les entreprises et les organisations qui envoient des e-mails au nom de plusieurs entités en aval à maintenir des profils de réputation distincts et à éviter que les problèmes liés à un client n'affectent les autres.

Qu'est-ce que la gestion des locataires ?

La gestion des locataires est une fonctionnalité qui vous permet de créer des conteneurs isolés appelés « locataires » au sein de votre compte SES. Chaque locataire peut avoir ses propres identités de messagerie, ensembles de configuration, modèles et indicateurs de réputation, ce qui garantit que les activités de courrier électronique sont complètement séparées entre les différents clients ou unités commerciales.

La gestion des locataires permet de relever le défi posé par le fait que les mauvaises pratiques d'un client en matière de courrier électronique pouvaient auparavant suspendre l'intégralité d'un compte SES, affectant ainsi tous les autres clients. Grâce à l'isolation des locataires, vous pouvez gérer plusieurs flux de courrier électronique de manière indépendante tout en maintenant une supervision et un contrôle centralisés.

Un locataire sert de conteneur logique qui regroupe les ressources SES associées. Lorsque vous envoyez des e-mails au nom d'un locataire spécifique, SES suit les indicateurs de réputation et applique les politiques au niveau du locataire. Cette isolation garantit qu'un taux de rebond élevé ou un taux de plaintes de la part d'un locataire n'a pas d'impact sur la délivrabilité des e-mails envoyés par les autres locataires.

La gestion des locataires est particulièrement utile pour :

- Les fournisseurs de logiciels indépendants (ISV) envoient des e-mails pour le compte de plusieurs clients.
- Entreprises gérant les communications par e-mail au sein de différentes unités commerciales.
- Les fournisseurs de services qui ont besoin d'isoler la réputation des e-mails par client ou par application.
- Organisations exigeant le respect de différentes exigences réglementaires par locataire.

Comment fonctionne la gestion des locataires

La gestion de la réputation des locataires fonctionne en créant un conteneur logique pour vos ressources d'envoi d'e-mails. Vous attribuez des ressources spécifiques à chaque locataire, notamment des identités vérifiées (domaines et adresses e-mail), des ensembles de configuration et des modèles. Lorsque vous envoyez un e-mail au nom d'un locataire, vous le spécifiez dans votre appel d'API ou dans votre en-tête SMTP, et SES vérifie que les ressources utilisées sont correctement associées à ce locataire.

Association de ressources

Les ressources de votre compte SES peuvent être associées aux locataires de deux manières :

- Mission dédiée — Ressources utilisées exclusivement par des locataires spécifiques.
- Affectation partagée : ressources disponibles pour plusieurs locataires.

Lorsque vous associez une ressource à un locataire, celui-ci obtient l'autorisation d'utiliser cette ressource pour envoyer des e-mails. À chaque demande d'envoi, SES vérifie que le locataire spécifié est autorisé à utiliser l'identité, le jeu de configuration et le modèle contenus dans la demande. Si les ressources ne sont pas correctement associées, la demande d'envoi échoue.

Surveillance et application de la réputation

SES surveille en permanence les principaux indicateurs de réputation de chaque locataire, notamment les taux de rebond, les taux de plaintes (y compris ceux provenant du système Feedback Loop (FBL) du fournisseur de boîtes aux lettres) et les signaux de feedback provenant de tiers. Lorsque ces indicateurs dépassent les seuils définis, SES crée des « résultats de réputation » classés comme suit :

- Avertissements de faible gravité : problèmes mineurs susceptibles d'affecter la délivrabilité s'ils ne sont pas résolus.
- Avertissements de gravité élevée : problèmes graves susceptibles d'affecter la délivrabilité et susceptibles de déclencher l'application de la loi.

Sur la base de ces résultats, SES peut automatiquement suspendre les locataires problématiques grâce à des politiques de réputation que vous configurez. Trois niveaux d'application sont disponibles :

- **Standard (recommandé)** — Suspend automatiquement l'envoi de locataires lorsque des résultats de réputation très graves sont détectés. Cela fournit une protection équilibrée tout en minimisant les perturbations.
- **Stricte** — Suspend automatiquement l'envoi des locataires lorsqu'une découverte de réputation est détectée, y compris des problèmes de faible gravité. Fournit une protection maximale, mais peut entraîner des pauses plus fréquentes.
- **Aucune** : désactive la pause automatique pour le locataire. Toutes les constatations relatives à la réputation sont toujours enregistrées et visibles, mais aucune mesure coercitive automatisée n'est prise.

Lorsque les statistiques d'un locataire déclenchent une constatation de réputation qui atteint le seuil d'application de la politique que vous avez sélectionnée, le système met automatiquement à jour le statut d'envoi du locataire sur « Suspendu » sans affecter la capacité d'envoi des autres locataires. Lorsqu'un locataire est suspendu, toute tentative d'envoi d'e-mail par ce locataire échouera tant que vous n'aurez pas examiné le problème et réactivé manuellement l'envoi. En outre, vous pouvez suspendre manuellement les fonctionnalités d'envoi d'un locataire en cas de besoin et les annuler lorsque vous êtes prêt à reprendre l'envoi.

Configuration des locataires

Rubriques

- [Création de locataires](#)
- [Affectation de ressources à un locataire](#)
- [Configuration des politiques de réputation](#)

Création de locataires

À l'aide de la console :

1. Connectez-vous à la console AWS de gestion et ouvrez la console SES à l'adresse <https://console.aws.amazon.com/ses/>.
2. Dans le volet de navigation, sélectionnez Tenants.
3. Choisissez Create tenant.
4. Dans Nom du locataire, entrez un nom unique pour votre locataire.
5. Choisissez Create tenant.

En utilisant AWS CLI :

```
aws sesv2 create-tenant \  
  --tenant-name "MyTenant" \  
  --region us-east-1
```

Affectation de ressources à un locataire

Après avoir créé un locataire, vous devez attribuer au moins une identité vérifiée et un ensemble de configuration avant que le locataire puisse envoyer un e-mail.

À l'aide de la console :

1. Dans la console SES, accédez à la page Tenants.
2. Sélectionnez le locataire que vous souhaitez configurer.
3. Dans la section Configuration du locataire, vous pouvez utiliser les cartes Identités et ensembles de configuration pour attribuer ces ressources. Vous pouvez éventuellement faire défiler l'écran jusqu'à la section à onglets et utiliser les onglets Identités et Ensembles de configuration pour faire de même.

Note

Toute tentative de suppression d'une identité ou d'un ensemble de configuration associé à un locataire échouera. Vous devez d'abord supprimer ces associations du locataire avant de pouvoir supprimer les ressources associées.

4. (Facultatif) Vous pouvez attribuer un ou plusieurs tags à votre locataire en sélectionnant l'onglet Tags.

En utilisant AWS CLI :

```
# Assign an identity to a tenant  
aws sesv2 create-tenant-resource-association \  
  --tenant-name "MyTenant" \  
  --resource-arn "arn:aws:ses:us-east-1:123456789012:identity/example.com" \  
  --region us-east-1  
  
# Assign a configuration set to a tenant  
aws sesv2 create-tenant-resource-association \  
  --tenant-name "MyTenant" \  
  --resource-arn "arn:aws:ses:us-east-1:123456789012:configuration-set/example.com" \  
  --region us-east-1
```

```
--tenant-name "MyTenant" \  
--resource-arn "arn:aws:ses:us-east-1:123456789012:configuration-set/MyConfigSet" \  
--region us-east-1
```

Configuration des politiques de réputation

Les politiques de réputation déterminent à quel moment l'envoi d'e-mails d'un locataire est automatiquement suspendu en fonction des indicateurs de réputation. Lorsque vous créez un locataire, SES attribue automatiquement la politique de réputation standard. Suivez les étapes ci-dessous si vous souhaitez passer à une autre politique.

À l'aide de la console :

1. Dans la console SES, accédez à la page Tenants.
2. Sélectionnez le locataire que vous souhaitez configurer.
3. Dans la section Configuration du locataire, vous pouvez utiliser la carte de politique de réputation pour attribuer une politique. Vous pouvez éventuellement faire défiler l'écran jusqu'à la section à onglets et utiliser l'onglet Politique de réputation pour faire de même.
4. Sélectionnez l'une des politiques suivantes :
 - Standard (recommandé) — Suspendez l'envoi lorsque des résultats très graves sont détectés.
 - Stricte — Suspendez l'envoi lorsque des résultats (y compris de faible gravité) sont détectés.
 - Aucun — Ne suspendez pas automatiquement l'envoi, quels que soient les résultats. Ce niveau comporte des risques, comme expliqué dans [Confiance et sécurité](#).

En utilisant AWS CLI :

```
update-reputation-entity-policy \  
  --reputation-entity-type "RESOURCE" \  
  --reputation-entity-reference "arn:aws:ses:us-east-1:123456789012:tenant/tenantId" \  
  --reputation-entity-policy "arn:aws:ses:us-east-1:aws:reputation-policy/standard"
```

Envoi d'un e-mail aux locataires

Lorsque vous envoyez un e-mail via un tenant, vous devez le spécifier dans vos appels d'API ou vos en-têtes SMTP et vous assurer que toutes les ressources utilisées sont associées à ce locataire.

Rubriques

- [Utilisation de l' SendEmail API avec les locataires](#)
- [Utilisation du protocole SMTP avec les locataires](#)

Utilisation de l' SendEmail API avec les locataires

AWS CLI Exemple :

```
aws sesv2 send-email \  
  --tenant-name "MyTenant" \  
  --from-email-address "sender@example.com" \  
  --destination "ToAddresses=recipient@example.com" \  
  --content "Simple={Subject={Data='Test Subject',Charset=utf-8},Body={Text={Data='Test  
email body',Charset=utf-8}}}" \  
  --configuration-set-name "MyConfigSet"
```

AWS Exemple de SDK pour Python :

```
import boto3  
  
client = boto3.client('sesv2')  
response = client.send_email(  
    FromEmailAddress='sender@example.com',  
    Destination={  
        'ToAddresses': ['recipient@example.com']  
    },  
    Content={  
        'Simple': {  
            'Subject': {  
                'Data': 'Test email'  
            },  
            'Body': {  
                'Text': {  
                    'Data': 'This is a test email sent using a tenant.'  
                }  
            }  
        }  
    },  
    ConfigurationSetName='MyConfigurationSet',  
    TenantName='MyTenant'  
)
```

Utilisation du protocole SMTP avec les locataires

Lorsque vous utilisez le protocole SMTP pour envoyer un e-mail via un locataire, incluez les informations du locataire dans un en-tête d'e-mail :

```
X-SES-TENANT: MyTenant
```

Cet en-tête indique à SES quel locataire doit être utilisé pour l'opération d'envoi d'e-mails, ce qui permet à SES d'appliquer la validation des ressources et le suivi de réputation appropriés.

Gestion du statut des locataires

Rubriques

- [Afficher le statut et les statistiques des locataires](#)
- [Suspendre et annuler la suspension des locataires](#)

Afficher le statut et les statistiques des locataires

À l'aide de la console :

1. Dans la console SES, accédez à la page Tenants.
2. Sélectionnez un locataire pour en afficher les détails.
3. La zone État du locataire affiche :

État de l'envoi :

- **Activé** — Le locataire peut envoyer des e-mails.
- **Suspendu** : vos politiques automatisées ou celles de SES ont suspendu l'envoi pour ce locataire.
- **Appliqué** — SES a suspendu ses envois en raison de graves problèmes de réputation.
- **Rétabli** — L'envoi a été réactivé après avoir été suspendu.

État de réputation :

- **Aucun résultat détecté** — Aucun problème n'affecte la délivrabilité.

- Avertissement de faible gravité : problèmes mineurs susceptibles d'affecter la délivrabilité s'ils ne sont pas résolus.
 - Avertissement de gravité élevée : problèmes graves susceptibles d'affecter la délivrabilité.
4. Faites défiler la page jusqu'à Statistiques d'envoi sous l'onglet Ressources pour consulter les statistiques de livraison, de rebond et de réclamation pour la plage de dates sélectionnée.

En utilisant AWS CLI :

```
# Get tenant details
aws sesv2 get-tenant --tenant-name "MyTenant"
```

Suspendre et annuler la suspension des locataires

Vous pouvez suspendre manuellement les fonctionnalités d'envoi d'un locataire en cas de besoin et les annuler lorsque vous êtes prêt à reprendre l'envoi.

À l'aide de la console :

1. Dans la console SES, accédez à la page Tenants.
2. Cochez la case à côté du locataire que vous souhaitez suspendre ou annuler.
3. Choisissez Suspendre l'envoi ou Reprendre l'envoi.
4. Confirmez l'action.

En utilisant AWS CLI :

Pour suspendre un locataire :

```
# Pause a tenant
aws sesv2 update-reputation-entity-customer-managed-status \
  --reputation-entity-type RESOURCE
  --reputation-entity-reference "arn:aws:ses:us-east-1:593442965613:tenant/tenantId"
  --sending-status DISABLED
```

Pour annuler la pause d'un locataire :

```
# Unpause a tenant
aws sesv2 update-reputation-entity-customer-managed-status \
```

```
--reputation-entity-type RESOURCE
--reputation-entity-reference "arn:aws:ses:us-east-1:593442965613:tenant/tenantId"
--sending-status ENABLED
```

Travailler avec les résultats de réputation

Rubriques

- [Afficher les résultats de réputation](#)
- [Comprendre les résultats relatifs à la réputation](#)
- [Résoudre les problèmes de réputation](#)

Afficher les résultats de réputation

À l'aide de la console :

1. Dans la console SES, accédez à la page Tenants.
2. Sélectionnez le locataire que vous souhaitez examiner.
3. Accédez au tableau des résultats de réputation.
4. Passez en revue tous les résultats actifs, y compris leur type, leur gravité, leur date de détection et les conseils pour résoudre le problème.

En utilisant AWS CLI :

```
aws sesv2 list-recommendations \
  --filter='{ "RESOURCE_ARN":"arn:aws:ses:us-east-1:012345678901:tenant/tenantId"}'
```

La réponse inclut des détails sur tous les résultats actifs :

```
{
  "Recommendations": [
    {
      "ResourceArn": "arn:aws:ses:us-east-1:012345678901:tenant/{tenant-name}/
{tenant-id}",
      "Type": "BOUNCE",
      "Description": "The bounce rate exceeded 15.0% based on a representative
volume of 664 emails from July 11, 2025 at 14:41 (UTC) to July 11, 2025 at 16:26
(UTC).",
```



```
        "Status": "OPEN",
        "CreatedTimestamp": "2025-07-11T16:16:14.029000+00:00",
        "LastUpdatedTimestamp": "2025-07-11T16:37:14.145000+00:00",
        "Impact": "HIGH"
    }
]
```

Comprendre les résultats relatifs à la réputation

Les résultats de réputation fournissent des informations sur les problèmes potentiels liés aux pratiques d'envoi d'e-mails de vos locataires. Chaque résultat inclut :

- Impact : niveau de gravité (élevé ou faible).
- Type de recherche : taux de rebond, taux de plaintes, commentaires de tiers provenant de fournisseurs de boîtes aux lettres et listes d'adresses IP bloquées.
- Âge : temps écoulé depuis la première date de détection.
- Description — Contexte du problème (tel que le taux spécifique qui a déclenché la découverte).
- Dernière vérification : date de la dernière mise à jour du statut.
- Résolution du problème : liens vers la section correspondante du guide du développeur SES contenant des conseils pour vous aider à résoudre le problème.

Les résultats courants incluent :

- Taux de rebond élevés : lorsque les taux de rebond dépassent les seuils configurés.
- Activité liée aux plaintes : lorsque des rapports de spam provenant de fournisseurs de boîtes aux lettres dépassent les seuils.
- Third-party feedback — Signaux négatifs émis par les fournisseurs de boîtes aux lettres.
- Apparences sur une liste de blocage — Lorsque vous envoyez des adresses IP, elles apparaissent sur une liste de blocage de réputation.

Résoudre les problèmes de réputation

Lorsque vous recevez une constatation de réputation, il est important d'en rechercher la cause première et de prendre rapidement des mesures correctives :

1. Traitez la cause première : conseillez à votre locataire d'améliorer l'hygiène des listes, de mettre à jour le contenu des e-mails ou de résoudre les problèmes techniques.
2. Passez en revue les pratiques d'envoi : assurez-vous que votre locataire respecte les meilleures pratiques en matière de courrier électronique.
3. Surveillez les indicateurs : surveillez l'amélioration des taux de rebond et de plaintes.
4. Communiquer avec les parties concernées — Informer les parties prenantes concernées du problème et des étapes de résolution.

Surveillance et analytique

Rubriques

- [Configuration des CloudWatch métriques](#)
- [Configuration des EventBridge notifications](#)

Configuration des CloudWatch métriques

SES publie des statistiques spécifiques aux locataires sur Amazon. CloudWatch Les mesures suivantes sont disponibles pour chaque locataire :

- Envois : nombre total d'e-mails envoyés par le locataire.
- Rebonds : nombre d'e-mails renvoyés par le locataire.
- Réclamations — Nombre de courriels renvoyés par le locataire.

Accès aux statistiques des locataires dans CloudWatch :

1. Ouvrez la CloudWatch console à l'adresse <https://console.aws.amazon.com/cloudwatch/>.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Sélectionnez l'espace de noms AWS/SSE.
4. Choisissez Par TenantId et TenantName pour afficher les statistiques spécifiques au locataire.

Configuration des EventBridge notifications

Par défaut, SES envoie des événements au bus d'événements EventBridge par défaut lorsque des informations relatives à la réputation du locataire sont détectées ou lorsque le statut du locataire change.

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.

Les types de détails suivants sont disponibles :

Pour les modifications de statut envoyées par le locataire :

- `Sending Status Enabled`— Le locataire est activé et peut envoyer des e-mails.
- `Sending Status Disabled`— Le locataire a été suspendu et ne peut pas envoyer d'e-mail.

Pour les résultats relatifs à la réputation :

- `Advisor Recommendation Status Open`
- `Advisor Recommendation Status Closed`

Configuration des EventBridge règles

1. Ouvrez la EventBridge console Amazon à l'adresse <https://console.aws.amazon.com/events/>.
2. Choisissez Créer une règle.
3. Saisissez un nom et une description pour la règle.
4. Pour Define pattern (Définir un modèle), sélectionnez Event pattern (Modèle d'événement).
5. Choisissez Pre-defined le modèle par service.
6. Choisissez SES comme nom de service.
7. Pour le type d'événement, choisissez État d'envoi activé ou État d'envoi désactivé.
8. Configurez le modèle d'événements pour qu'il corresponde aux événements spécifiques qui vous intéressent.
9. Choisissez votre cible (telle qu'une fonction AWS Lambda, une rubrique Amazon SNS ou une file d'attente Amazon SQS).
10. Configurez tous les paramètres supplémentaires nécessaires.

11. Choisissez Créer.

Exemple de modèle de EventBridge règles pour les résultats de réputation :

```
{
  "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:tenant/{tenant-name}/{tenant-id}"
  ],
  "detail": {
    "version": "1.0.0",
    "data": "The bounce rate exceeded 15.0% based on a representative volume of 197 emails from July 11, 2025 at 14:43 (UTC) to July 11, 2025 at 16:13 (UTC).",
    "metadata":{"impact":"HIGH","type":"BOUNCE"}
  }
}
```

Exemple de modèle de EventBridge règle pour l'envoi de modifications de statut :

```
{
  "detail-type": "Sending Status Disabled",
  "source": "aws.ses",
  "account": "012345678901",
  "time": "2025-07-24T12:44:28Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ses:us-east-1:012345678901:tenant/{tenant-name}/{tenant-id}"
  ],
  "detail": {
    "version": "1.0.0",
    "data": {
      "origin": "CUSTOMER_MANAGED",
      "record": {
        "status": "DISABLED",
        "cause": "Status manually updated.",
        "lastUpdatedTimestamp": [2025, 7, 24, 12, 44, 28, 995000000]
      }
    }
  }
}
```

```
    }  
  }  
}
```

Descriptions des champs :

- `source` — Identifie le service qui a généré l'événement. Pour les événements SES, cette valeur est `aws.ses`.
- `detail-type` — Type d'événement de changement de statut (voir Types d'événements ci-dessus).
- `resources` — Tableau contenant l'ARN du locataire concerné.
- `detail.data.origin` — Source du changement de statut (par exemple, « `CUSTOMER_MANAGED` » ou « `AWS_MANAGED` »).
- `detail.data.record.status` — Le nouveau statut du locataire (ACTIVÉ, DÉSACTIVÉ ou RÉTABLI).
- `detail.data.record.cause` — Description de la raison pour laquelle le statut a changé.
- `detail.data.record.last UpdatedTimestamp` — Horodatage de la mise à jour du statut.

Vous pouvez utiliser ces événements pour surveiller les changements de statut des locataires et automatiser les réponses dans vos applications. Par exemple, vous souhaitez peut-être déclencher des alertes lorsque les locataires sont désactivés ou suivre les indicateurs de santé des locataires au fil du temps.

Intégration à AWS Confiance & et sécurité

Lorsque AWS Trust & Safety détecte des problèmes qui devraient normalement entraîner une application au niveau du compte, le système des locataires permet des réponses plus ciblées. Au lieu de suspendre l'intégralité de votre compte, Trust & Safety peut suspendre uniquement les locataires problématiques tout en permettant aux locataires conformes de continuer à envoyer.

Cette application au niveau du locataire réduit l'impact des problèmes de réputation et permet de maintenir la continuité des activités pour vos autres flux de courrier électronique.

Vous recevrez des notifications lorsque SES aura désactivé l'envoi en raison de problèmes graves affectant la réputation du locataire et aura soumis votre compte à un examen. Un dossier vous sera ouvert dans le AWS Support Center afin que vous puissiez travailler avec Trust & Safety pour résoudre les problèmes et rétablir l'envoi pour le locataire concerné.

 Note

En tant que propriétaire du compte, il est de votre responsabilité de surveiller les indicateurs de réputation de tous vos locataires. Bien que la fonctionnalité des locataires isole le suivi de la réputation au niveau du locataire, leur activité d'envoi combinée a toujours une incidence sur la réputation globale de votre compte. Les locataires qui adoptent de mauvaises pratiques d'envoi peuvent mettre en danger l'ensemble de votre compte. Il est donc essentiel de s'assurer que tous les locataires appliquent de bonnes pratiques d'envoi d'e-mails afin de protéger le statut de votre compte.

Bonnes pratiques

Suivez ces bonnes pratiques pour gérer efficacement la réputation des locataires dans Amazon SES :

- Commencez par la politique standard : pour la plupart des locataires, la politique de réputation standard fournit un bon équilibre entre protection et stabilité opérationnelle.
- Surveiller avant d'appliquer : lors de l'intégration de nouveaux locataires, envisagez d'utiliser temporairement la politique « Aucun » tout en surveillant leurs habitudes d'envoi (par exemple avec EventBridge) avant d'activer l'application automatique.
- Configurez EventBridge des notifications : créez des alertes relatives aux résultats de réputation afin de prendre des mesures proactives avant qu'une pause automatique ne se produise.
- Passez régulièrement en revue les statistiques relatives aux locataires : surveillez les statistiques d'envoi au niveau des locataires, même en l'absence de résultats de réputation, afin d'identifier les tendances émergentes.
- Éduquez vos locataires — Fournissez des directives [Bonnes pratiques de messagerie électronique](#) pour aider les locataires à conserver une bonne réputation d'expéditeur.
- Appliquez les politiques appropriées — Appliquez la politique stricte aux locataires à haut risque ou à ceux qui ont des antécédents de problèmes de réputation.
- Réagissez rapidement aux résultats — Lorsqu'un résultat est détecté, étudiez immédiatement la cause première et prenez les mesures correctives appropriées.
- Planification des ressources — Concevez votre structure de locataires en fonction des besoins de votre entreprise. Les locataires peuvent représenter plusieurs clients (ISV), unités commerciales, client/application types et exigences réglementaires.

Tenant-level listes de suppression

Par défaut, tous les locataires de votre compte partagent la liste de suppression au niveau du compte. Cela signifie que lorsqu'un destinataire renvoie ou se plaint de l'adresse e-mail d'un locataire, cette adresse est supprimée pour tous les locataires du compte. Tenant-level les listes de suppression résolvent ce problème en donnant à chaque locataire sa propre liste de suppression isolée.

Lorsque vous activez la suppression au niveau du locataire pour un locataire, SES gère une liste de suppression distincte pour ce locataire. Les rebonds et les plaintes ne concernent que le locataire qui a envoyé l'e-mail. Les autres locataires peuvent continuer à envoyer aux mêmes destinataires. Vous configurez la suppression au niveau du locataire en définissant le `SuppressionScope` to `TENANT` et en choisissant lequel `SuppressedReasons` (rebonds, plaintes, ou les deux) à suivre.

Pour des informations complètes sur la configuration et la gestion des listes de suppression au niveau des locataires, consultez. [Utilisation de listes de suppression au niveau des locataires dans Amazon SES](#)

Limitations

Lorsque vous utilisez la gestion des locataires, tenez compte des limites suivantes :

- **Portée régionale** — Les locataires sont spécifiques à une région et ne sont pas automatiquement répliqués d'une région à l'autre. Régions AWS Si vous envoyez des e-mails depuis plusieurs régions, vous devrez configurer et surveiller la réputation des locataires séparément dans chaque région.
- **Limites de quotas** : par défaut, les comptes peuvent créer jusqu'à 10 000 locataires. Vous pouvez demander des augmentations via la console AWS Service Quota, avec une approbation automatique disponible jusqu'à 300 000 locataires pour les comptes éligibles.
- **Configuration requise** : lorsque vous envoyez pour le compte d'un locataire, vous devez spécifier un ensemble de configuration associé à ce locataire ou utiliser une identité associée à un ensemble de configuration par défaut associé au locataire.
- **Périodes de calcul des métriques** — Les métriques de réputation sont calculées en fonction de l'activité d'envoi récente, généralement sur une période continue de 24 à 7 jours selon le type de métrique.
- **Volume d'envoi minimal** — Certaines évaluations de réputation nécessitent un volume minimum représentatif d'e-mails avant de pouvoir être déclenchées.

- **Re-enabling période de grâce** — Après avoir réactivé un locataire suspendu, celui-ci entre dans un état de « réintégration » où les résultats de réputation actifs sont temporairement ignorés pour permettre au locataire de se rétablir. Le locataire restera dans cet état jusqu'à ce que toutes les conclusions actives soient résolues.
- **Cross-account limites** — Les locataires ne peuvent pas couvrir plusieurs AWS comptes. Chaque compte gère son propre ensemble de locataires de manière indépendante.
- **Pas de nidification des locataires** : les locataires ne peuvent pas contenir d'autres locataires, ce sont des structures plates.

Tarification

Des frais supplémentaires sont facturés par locataire et par mois en fonction du nombre de courriels. Pour obtenir des informations détaillées sur les tarifs, consultez la [page de tarification de SES](#).

Lors de l'utilisation CloudWatch avec les métriques des locataires, CloudWatch les métriques standard pour chaque locataire sont fournies sans frais supplémentaires dans le cadre de la surveillance de base. Des CloudWatch fonctionnalités supplémentaires telles que des tableaux de bord personnalisés, des alarmes ou une surveillance détaillée peuvent entraîner des frais standard CloudWatch.

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](#)
- [Vérification des identités dans Amazon SES](#)
- [Configuration des identités dans Amazon SES](#)
- [Envoi d'e-mails test dans Amazon SES avec le simulateur](#)

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 les fonctionnalités de vérification, d'héritage et d'envoi d'e-mails évoquées ci-dessus, le tableau suivant classe chaque combinaison de vérification d' domaine/email adresse et répertorie l'héritage, le niveau d'envoi et le statut d'affichage de chacune d'elles :

	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	Console/API statut : • Domain/Su bdomains = Vérifié • Adresse e-mail = Non vérifié.	Console/API statut : • Adresse e-mail = Vérifié	Console/API statut : • Domain/Su bdomains = 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 depuis le même domaine ou adresse e-mail dans plusieurs régions 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.exemple.com` (une adresse e-mail qui est vérifiée spécifiquement) utilisent les paramètres pour `utilisateur@a.b.exemple.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 `sender@example.com`, vous pouvez utiliser `sender+ myLabel@example.com` comme adresse « De » ou « » Return-Path 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 `EXAMPLE.com` également envoyer depuis.
- Les adresses e-mail sont sensibles à la casse. Si vous validez `sender@EXAMPLE.com`, vous ne pouvez pas envoyer d'e-mail depuis `sender@example.com` à moins de vérifier également `sender@example.com`.
- Dans chacune d'elles Région AWS, vous pouvez vérifier jusqu'à 10 000 identités (domaines et adresses e-mail, toutes combinaisons confondues).

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](#)
- [Vérification d'une identité de domaine DKIM auprès de votre fournisseur DNS](#)
- [Création d'une identité d'adresse e-mail](#)
- [Vérification d'une identité d'adresse e-mail](#)
- [Créez et vérifiez une identité et attribuez un jeu de configuration par défaut en même temps](#)
- [Utilisation de modèles d'e-mail de vérification personnalisé](#)

Création d'une identité de domaine

La création d'une identité de domaine consiste notamment à configurer sa DKIM-based vérification. DomainKeys Le courrier identifié (DKIM) est une méthode d'authentification des e-mails qu'Amazon SES utilise pour vérifier la propriété du domaine et que les serveurs de réception de courrier 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 console Amazon SES AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/ses/>.

2. Dans le volet de navigation, sous Configuration, choisissez Identities.
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 “Modifier une identité à l'aide de la console”](#).)
8. (Facultatif) Pour configurer la DKIM-based vérification personnalisée, autre que le paramètre par défaut de SES qui utilise [Easy DKIM](#) avec une longueur de signature de 2048 bits, sous Vérifier votre domaine, développez les paramètres DKIM avancés et choisissez le type de DKIM que vous souhaitez configurer :
- a. Easy DKIM :
 - i. Sous 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 “Modifier une identité à l'aide de la console”](#).)
 - b. DKIM facile déterministe (DEED) :

 Tip

Cette forme de DKIM doit être utilisée si vous créez une identité globale (réplique). DEED utilisera la configuration Easy DKIM d'une identité existante du même nom provenant d'une région parent et signera la nouvelle identité sans que vous ayez à effectuer de configuration DNS supplémentaire. Pour plus d'informations, consultez [DEED](#).

- i. Sous Type d'identité, choisissez Deterministic Easy DKIM.
 - ii. Dans le menu déroulant Région parent, sélectionnez une région parent dans laquelle réside une DKIM-signed identité Easy portant le même nom que celui que vous avez saisi pour votre identité globale (réplique). (La région de votre réplique correspond par défaut à la région avec laquelle vous vous êtes connecté à la console SES.)
- c. (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. Sous Type d'identité, choisissez 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.

 Note

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.

- Si vous avez créé une identité globale (réplique) à l'aide de Deterministic Easy DKIM (DEED), aucune configuration DNS supplémentaire n'est requise. Vous pouvez ignorer cette étape. Pour plus d'informations, consultez [DEED](#).

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 Authentication 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.

▼ Publish DNS records

After you've created your domain identity with Easy DKIM, you must complete the verification process with DKIM authentication by copying the following generated CNAME records to publish to your domain's DNS provider. Detection of these records may take up to 72 hours. For more information, see [Verifying a domain identity with DKIM](#) and [Easy DKIM](#).

Type	Name	Value
CNAME	a32gfwufpxmw36t5sf2owbszld3sof7_domainkey.adzel.com	a32gfwufpxmw36t5sf2owbszld3sof7.dkim.amazonses.com
CNAME	redmf6qg6wg3no6ulb6mrmwxjeypgpdh_domainkey.adzel.com	redmf6qg6wg3no6ulb6mrmwxjeypgpdh.dkim.amazonses.com
CNAME	6d5oug5am4wtxnkr4rdwluadqdd5l74l_domainkey.adzel.com	6d5oug5am4wtxnkr4rdwluadqdd5l74l.dkim.amazonses.com

[Download .csv record set](#)

Récupération de la zone hébergée par programmation

La valeur de chaque enregistrement CNAME est composée du jeton DKIM suivi d'un domaine de zone hébergé (par exemple, `token.dkim.amazonses.com` ou `token.a31d.dkim.us-west-2.amazonses.com`). La partie de la zone hébergée varie selon Région AWS les cellules.

Vous pouvez récupérer la zone hébergée directement depuis la réponse de l'API. Les [GetEmailIdentity](#) réponses [CreateEmailIdentity](#) et incluent toutes deux un `SigningHostedZone` champ dans l'`DkimAttributes` objet.

Utilisez cette valeur pour construire la valeur d'enregistrement CNAME complète : `token.SigningHostedZone`.

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. Consultez le [tableau des DNS/Hosting fournisseurs](#) 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 “Modifier 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.

▼ Publish DNS records

ⓘ After you've created your domain identity with BYODKIM by providing the private key from your self-generated public-private key pair, ensure the Selector name matches what's in your domain's DNS provider settings. ("p=customerProvidedPublicKey" is only a placeholder for the public key you supplied to your DNS provider.) Detection of these records may take up to 72 hours. For more information, see [Verifying a domain identity with DKIM](#) and [BYODKIM](#).

Type	Name	Value
TXT	myselector_domainkey.byodkim.adzel.com	p=customerProvidedPublicKey

[Download .csv record set](#)

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. Consultez le [tableau des DNS/Hosting fournisseurs](#) 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 le tableau Publier les enregistrements DNS, l'enregistrement de clé publique qui apparaît dans la colonne Valeur affiche uniquement « p= customer ProvidedPublicKey » comme espace réservé pour la valeur de 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).

 Tip

Lorsque vous ajoutez des enregistrements CNAME à votre configuration DNS :

- Utilisez les noms d'enregistrement exacts tels qu'ils sont fournis dans la console SES.

- N'ajoutez aucun trait de soulignement (_) supplémentaire au début des noms d'enregistrement CNAME.
- La `_domainkey` partie fait partie du nom de l'enregistrement et doit être utilisée exactement comme indiqué.

Exemple montrant une implémentation correcte ou incorrecte de l'enregistrement CNAME :

- Correct : `abc123._domainkey.domain.com`
- Incorrect : `_abc123._domainkey.domain.com`

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.

DNS/Hosting fournisseur	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)

DNS/Hosting fournisseur	Lien vers la documentation
HostGator	Gérer les enregistrements DNS avec HostGator /eNom (lien externe)
Namecheap	Comment ajouter TXT/SPF/DKIM/DMARC des enregistrements 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 de DNS appellent ce Name/hostchamp Host ou Hostname. 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 automatiquement ajouté votre nom de domaine à la Name/hostvaleur que vous avez saisie dans l'enregistrement 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 Name/hostvaleur, 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 caractère de soulignement (_) est obligatoire dans la Name/hostvaleur de chaque enregistrement 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 enregistrements de validation que vous devez ajouter aux paramètres DNS de votre domaine sont différents pour chacun Région AWS. Si vous souhaitez utiliser un domaine pour envoyer

des e-mails depuis plusieurs régions Régions AWS, vous devez créer et vérifier une identité de domaine distincte pour 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 console Amazon SES AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/ses/>.
2. Dans le volet de navigation, sous Configuration, choisissez Identities.
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'[CreateEmailIdentity](#) opération dans l'API Amazon SES v2 pour créer une nouvelle identité e-mail et définir sa configuration par défaut en même temps.

Note

Avant d'effectuer la procédure complète décrite dans cette section, vous devez installer et configurer l'AWS CLI. Pour plus d'informations, consultez le [Guide de l'utilisateur AWS Command Line Interface](#).

Pour définir un ensemble de configuration par défaut à l'aide du AWS CLI

- Sur la ligne de commande, entrez la commande suivante pour utiliser l'[CreateEmailIdentity](#) opération.

```
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 e-mail que vous souhaitez vérifier. *CONFIG-SET* Remplacez-le par le nom du jeu de configuration que vous souhaitez définir comme jeu de configuration 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 dont l'objet est le suivant : « Amazon Web Services - Demande de vérification d'adresse e-mail dans la région »*RegionName*, où *RegionName* est le nom de la personne dans Région AWS 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=TJDuffhYYK1fSHCSBq4cbodBQq%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 <code>FromEmailAddress</code> 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.
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 AWS SDK ou le AWS CLI pour créer un modèle d'e-mail de vérification personnalisé avec l'`CreateCustomVerificationEmailTemplate` opération. Pour en savoir plus sur les AWS SDK, consultez la section [Outils pour Amazon Web Services](#). Pour plus d'informations sur le AWS CLI, voir [Interface de ligne de AWS commande](#).

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 plus d'informations sur l'installation et la configuration du AWS CLI, consultez le [guide de AWS Command Line Interface l'utilisateur](#).

 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 la mise à jour du AWS CLI, consultez la section [Installation du AWS Command Line Interface](#) dans le guide de AWS Command Line Interface l'utilisateur.

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

Après avoir créé au moins un modèle d'e-mail de vérification personnalisé, vous pouvez l'envoyer à vos clients en appelant l'opération [SendCustomVerificationEmail](#) API. Vous pouvez appeler l'opération SendCustomVerificationEmail à l'aide de l'un des AWS SDK ou du 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=TJDuffhYYK1fSHCSBq4qjbodBQq%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 : ``

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
<code>abbr</code>	<code>class, id, style, title</code>
<code>acronym</code>	<code>class, id, style, title</code>
<code>address</code>	<code>class, id, style, title</code>
<code>area</code>	<code>class, id, style, title</code>
<code>b</code>	<code>class, id, style, title</code>
<code>bdo</code>	<code>class, id, style, title</code>
<code>big</code>	<code>class, id, style, title</code>

Balise HTML	Attributs autorisés
<code>blockquote</code>	<code>cite, class, id, style, title</code>
<code>body</code>	<code>class, id, style, title</code>
<code>br</code>	<code>class, id, style, title</code>
<code>button</code>	<code>class, id, style, title</code>
<code>caption</code>	<code>class, id, style, title</code>
<code>center</code>	<code>class, id, style, title</code>
<code>cite</code>	<code>class, id, style, title</code>
<code>code</code>	<code>class, id, style, title</code>
<code>col</code>	<code>class, id, span, style, title, width</code>
<code>colgroup</code>	<code>class, id, span, style, title, width</code>
<code>dd</code>	<code>class, id, style, title</code>
<code>del</code>	<code>class, id, style, title</code>
<code>dfn</code>	<code>class, id, style, title</code>
<code>dir</code>	<code>class, id, style, title</code>
<code>div</code>	<code>class, id, style, title</code>
<code>dl</code>	<code>class, id, style, title</code>
<code>dt</code>	<code>class, id, style, title</code>
<code>em</code>	<code>class, id, style, title</code>
<code>fieldset</code>	<code>class, id, style, title</code>

Balise HTML	Attributs autorisés
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
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

Balise HTML	Attributs autorisés
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
sub	class, id, style, title
sup	class, id, style, title
table	class, id, style, summary, title, width
tbody	class, id, style, title

Balise HTML	Attributs autorisés
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 comporter jusqu'à 10 000 identités vérifiées dans chaque AWS région. 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. S'agit-il d'e-mails de vérification personnalisés DKIM-signed ?

Pour que les e-mails de vérification soient valides DKIM-signed, l'adresse e-mail que vous spécifiez dans l'`FromEmailAddress` attribut lorsque vous créez le 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 SDK ou le AWS CLI, vous utilisez peut-être une ancienne version du 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 du AWS Command Line Interface
- Version 3.3.205.0 ou ultérieure du AWS SDK pour .NET
- Version 1.3.20170531.19 ou ultérieure du SDK pour C++AWS

- Version 1.12.43 ou ultérieure du AWS SDK pour Go
- Version 1.11.245 ou ultérieure du AWS SDK pour Java
- Version 2.166.0 ou ultérieure du AWS SDK pour JavaScript
- Version 3.45.2 ou ultérieure du AWS SDK pour PHP
- Version 1.5.1 ou ultérieure du AWS SDK pour Python (Boto)
- Version 1.5.0 ou ultérieure de la gem `aws-sdk-ses` dans AWS SDK pour 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 consulter les identités que vous avez créées pour chacune Région AWS, ouvrir une identité pour voir et modifier ses paramètres détaillés, associer un ensemble de configuration par défaut ou supprimer une ou plusieurs identités.

Note

Les procédures référencées dans cette section s'appliquent uniquement aux identités de la zone sélectionnée Région AWS. Pour gérer les identités créées dans plusieurs régions, répétez les procédures pour chacune d'entre elles Région AWS.

Table des matières

- [Afficher les identités à l'aide de la console SES](#)
- [Supprimer une identité à l'aide de la console SES](#)
- [Modifier une identité à l'aide de la console SES](#)
- [Modifier une identité pour utiliser un ensemble de configuration par défaut à l'aide de l'API SES](#)
- [Récupérez le jeu de configuration par défaut utilisé par l'identité à l'aide de l'API SES](#)
- [Remplacer l'ensemble de configuration par défaut actuel utilisé par l'identité à l'aide de l'API SES](#)

Afficher les identités à l'aide de la console SES

Vous pouvez utiliser la console Amazon SES pour consulter les identités de domaine et d'adresse e-mail vérifiées ou en attente 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

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 la console, utilisez le sélecteur de région pour choisir celle Région AWS pour laquelle vous souhaitez consulter 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 :
 - Vérifié (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.

Supprimer une identité à l'aide de la console SES

Vous pouvez utiliser la console Amazon SES pour supprimer une identité de domaine ou d'adresse e-mail de votre compte dans le champ sélectionné Région AWS.

Pour supprimer une identité de domaine ou d'adresse e-mail

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 la console, utilisez le sélecteur de région pour choisir Région AWS celle dont 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 (Supprimer).

Modifier une identité à l'aide de la console SES

Vous pouvez utiliser la console Amazon SES pour modifier l'identité d'un domaine ou d'une adresse e-mail dans le compte sélectionné Région AWS.

Pour modifier l'identité d'un domaine ou d'une adresse e-mail

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 la console, utilisez le sélecteur de région pour choisir celle à Région AWS partir de 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 les attributs sous l'onglet Authentication et que votre identité de domaine est hébergée sur Amazon Route 53, et que vous n'avez pas encore publié ses enregistrements DNS, un bouton Publier les enregistrements DNS sur Route53 (à côté du bouton Modifier) apparaîtra dans l'un ou l'autre des conteneurs de domaine DomainKeys Identified Mail (DKIM) ou Custom MAIL FROM.
7. Répétez les étapes 5 et 6 pour chaque attribut de l'identité que vous souhaitez modifier.

 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.

Modifier une identité pour utiliser un ensemble de configuration par défaut à l'aide de l'API SES

Vous pouvez utiliser cette [PutEmailIdentityConfigurationSetAttributes](#) opération pour ajouter ou supprimer un ensemble de configuration par défaut à partir d'une identité de messagerie existante.

 Note

Avant d'effectuer la procédure complète décrite dans cette section, vous devez installer et configurer l' AWS CLI. Pour plus d'informations, consultez le [Guide de l'utilisateur AWS Command Line Interface](#).

Pour ajouter un ensemble de configuration par défaut à l'aide du AWS CLI

- Sur la ligne de commande, entrez la commande suivante pour utiliser l'[PutEmailIdentityConfigurationSetAttributes](#) opération.

```
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 e-mail que vous souhaitez vérifier. *CONFIG-SET* Remplacez-le par le nom du jeu de configuration que vous souhaitez définir comme jeu de configuration par défaut de l'identité.

Si la commande s'exécute correctement, elle se termine sans fournir de sortie.

Pour supprimer un ensemble de configuration par défaut à l'aide du AWS CLI

- Sur la ligne de commande, entrez la commande suivante pour utiliser l'[PutEmailIdentityConfigurationSetAttributes](#) opération.

```
aws sesv2 put-email-identity-configuration-set-attributes --email-identity ADDRESS-OR-  
DOMAIN
```

Dans les commandes précédentes, remplacez *ADDRESS-OR-DOMAIN* par l'identité e-mail que vous souhaitez vérifier.

Si la commande s'exécute correctement, elle se termine sans fournir de sortie.

Récupérez le jeu de configuration par défaut utilisé par l'identité à l'aide de l'API SES

Vous pouvez utiliser cette [GetEmailIdentity](#) opération pour renvoyer la configuration par défaut définie pour une identité de messagerie, le cas échéant.

Note

Avant d'effectuer la procédure complète décrite dans cette section, vous devez installer et configurer l' AWS CLI. Pour plus d'informations, consultez le [Guide de l'utilisateur AWS Command Line Interface](#).

Pour renvoyer un ensemble de configuration par défaut à l'aide du AWS CLI

- Sur la ligne de commande, entrez la commande suivante pour utiliser l'[GetEmailIdentity](#) opération.

```
aws sesv2 get-email-identity --email-identity ADDRESS-OR-DOMAIN
```

Dans les commandes précédentes, remplacez par *ADDRESS-OR-DOMAIN* par l'identité e-mail pour laquelle vous souhaitez connaître la configuration par défaut définie, 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 l'ensemble de configuration par défaut actuel utilisé par l'identité à l'aide de l'API SES

Vous pouvez utiliser cette [SendEmail](#) opération pour envoyer un e-mail avec un ensemble de configuration 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 plus d'informations, consultez le [Guide de l'utilisateur AWS Command Line Interface](#).

Pour remplacer un ensemble de configuration par défaut à l'aide du AWS CLI

- Sur la ligne de commande, entrez la commande suivante pour utiliser l'[SendEmail](#) opération.

```
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 configuration que vous souhaitez utiliser au lieu de celui défini 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 ISPs entreprises qui redirigent le trafic de courrier électronique prennent des mesures pour évaluer si le courrier électronique est légitime. L'une de ces ISPs mesures 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, ISPs refusez 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 ISPs utilisés, le Sender Policy Framework (SPF) et le courrier DomainKeys identifié (DKIM), et fournissent des instructions sur l'utilisation de 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 DKIM, une norme qui vous permet de signer vos e-mails afin de montrer aux ISPs que vos messages sont légitimes et qu'ils n'ont pas été modifiés pendant le transport, 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 ISPs entreprises qui redirigent le trafic de courrier électronique prennent des mesures pour évaluer si le courrier électronique est légitime. L'une de ces mesures 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 ISPs 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](#)
- [Authentification d'e-mails avec SPF dans Amazon SES](#)
- [Utilisation d'un domaine MAIL FROM personnalisé](#)
- [Mise en conformité au protocole d'authentification DMARC dans Amazon SES](#)
- [Utilisation de BIMI dans Amazon SES](#)

Authentification d'e-mails avec DKIM dans Amazon SES

DomainKeys Le courrier identifié (DKIM) est une norme de sécurité du courrier électronique conçue pour garantir qu'un e-mail prétendant 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](#).
- Deterministic Easy DKIM (DEED) : vous permet de maintenir une signature DKIM cohérente sur plusieurs Régions AWS en créant des répliques d'identités qui héritent automatiquement des attributs de signature DKIM en tant qu'identité parent utilisant Easy DKIM, voir. [Utilisation de Deterministic Easy DKIM \(DEED\) 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 AWS régions. 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 console Amazon SES AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/ses/>.
2. Dans le volet de navigation, sous Configuration, choisissez Identities.
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 DomainKeysIdentified Mail (DKIM), choisissez Modifier.
5. Dans le conteneur Advanced DKIM settings (Paramètres avancés de DKIM), choisissez le bouton Easy DKIM dans la zone Identity 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. Sélectionnez 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 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 celle pour laquelle vous souhaitez modifier la longueur de la clé de signature DKIM.
4. Sous l'onglet Authentification, dans le conteneur DomainKeysIdentified Mail (DKIM), choisissez 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. Sélectionnez Enregistrer les modifications.

Utilisation de Deterministic Easy DKIM (DEED) dans Amazon SES

Deterministic Easy DKIM (DEED) propose une solution pour gérer les configurations DKIM sur plusieurs Régions AWS. En simplifiant la gestion du DNS et en garantissant une signature DKIM cohérente, DEED vous aide à rationaliser vos opérations d'envoi d'e-mails dans plusieurs régions tout en maintenant de solides pratiques d'authentification des e-mails.

Qu'est-ce que Deterministic Easy DKIM (DEED) ?

Deterministic Easy DKIM (DEED) est une fonctionnalité qui génère des jetons DKIM cohérents dans tous les domaines sur la Région AWS base d'un domaine parent configuré avec Easy DKIM.

Cela vous permet de répliquer des identités différentes Régions AWS qui héritent et conservent automatiquement la même configuration de signature DKIM qu'une identité parent actuellement configurée avec Easy DKIM. Avec DEED, vous ne devez publier les enregistrements DNS qu'une seule fois pour l'identité du parent, et les identités répliquées utiliseront les mêmes enregistrements DNS pour vérifier la propriété du domaine et gérer la signature DKIM.

En simplifiant la gestion du DNS et en garantissant une signature DKIM cohérente, DEED vous aide à rationaliser vos opérations d'envoi d'e-mails dans plusieurs régions tout en respectant les meilleures pratiques d'authentification des e-mails.

Terminologie utilisée pour parler de DEED :

- Identité parent : identité vérifiée configurée avec Easy DKIM qui sert de source pour la configuration DKIM d'une réplique d'identité.
- Identité répliquée : copie d'une identité parent qui partage la même configuration DNS et la même configuration de signature DKIM.
- Région parent — L' Région AWS endroit où l'identité d'un parent est configurée.
- Région de réplication : zone Région AWS dans laquelle une identité de réplique est configurée.
- Identité DEED — Toute identité utilisée soit comme identité parent, soit comme identité de réplique. (Lorsqu'une nouvelle identité est créée, elle est initialement traitée comme une identité normale (autre que DEED). Cependant, une fois qu'une réplique est créée, l'identité est alors considérée comme une identité DEED.)

Les principaux avantages de l'utilisation de DEED sont les suivants :

- Gestion DNS simplifiée : publiez les enregistrements DNS une seule fois pour l'identité du parent.

- Simplification des opérations multirégionales — Simplifiez le processus d'extension des opérations d'envoi d'e-mails à de nouvelles régions.
- Réduction des frais administratifs : gérez les configurations DKIM de manière centralisée à partir de l'identité du parent.

Comment fonctionne Deterministic Easy DKIM (DEED)

Lorsque vous créez une identité de réplique, Amazon SES réplique automatiquement la clé de signature DKIM de l'identité parent vers l'identité de réplique. Toutes les rotations de touches DKIM ou les modifications de longueur de clé ultérieures apportées à l'identité parent sont automatiquement propagées à toutes les identités répliquées.

Le processus implique le flux de travail suivant :

1. Créez une identité de parent dans un Easy DKIM à Région AWS l'aide de Easy DKIM.
2. Configurez les enregistrements DNS requis pour l'identité du parent.
3. Créez des répliques d'identités dans d'autres Régions AWS, en spécifiant le nom de domaine et la région de signature DKIM de l'identité parent.
4. Amazon SES réplique automatiquement la configuration DKIM du parent sur les identités de réplication.

Considérations importantes :

- Vous ne pouvez pas créer une réplique d'une identité qui est déjà une réplique.
- [Easy DKIM doit être activé sur l'identité parent. Vous ne pouvez pas créer de répliques de BYODKIM](#) ou d'identités signées manuellement.
- Les identités parentes ne peuvent pas être supprimées tant que toutes les identités répliquées ne sont pas supprimées.

Configuration d'une identité dupliquée à l'aide de DEED

Cette section fournit des exemples vous montrant comment créer et vérifier une réplique d'identité à l'aide de DEED, ainsi que les autorisations nécessaires requises.

Rubriques

- [Création d'une identité répliquée](#)

- [Vérifier la configuration de l'identité des répliques](#)
- [Autorisations requises pour utiliser DEED](#)

Création d'une identité répliquée

Pour créer une identité de réplique :

1. Dans l' Région AWS endroit où vous souhaitez créer une réplique d'identité, ouvrez la console SES à l'adresse <https://console.aws.amazon.com/ses/>.

(Dans la console SES, les identités répliquées sont appelées identités globales.)
2. Dans le volet de navigation, sélectionnez Identities.
3. Choisissez Create identity (Créer une identité).
4. Sélectionnez Domaine sous Type d'identité et entrez le nom de domaine d'une identité existante configurée avec Easy DKIM que vous souhaitez répliquer et servir de parent.
5. Développez les paramètres DKIM avancés et sélectionnez Deterministic Easy DKIM.
6. Dans le menu déroulant Région parent, sélectionnez une région parent dans laquelle réside une identité signée Easy DKIM portant le même nom que celui que vous avez saisi pour votre identité globale (réplique). (La région de votre réplique correspond par défaut à la région avec laquelle vous vous êtes connecté à la console SES.)
7. Assurez-vous que les signatures DKIM sont activées.
8. (Facultatif) Ajoutez une ou plusieurs balises à l'identité de votre domaine.
9. Passez en revue la configuration et choisissez Create identity.

En utilisant AWS CLI :

Pour créer une identité de réplique basée sur une identité parent configurée avec Easy DKIM, vous devez spécifier le nom de domaine du parent, la région dans laquelle vous souhaitez créer l'identité de réplique et la région de signature DKIM du parent, comme indiqué dans cet exemple :

```
aws sesv2 create-email-identity --email-identity example.com --region us-west-2 --dkim-signing-attributes '{"DomainSigningAttributesOrigin": "AWS_SES_US_EAST_1"}'
```

Dans l'exemple précédent :

1. Remplacez *example.com* par l'identité du domaine parent en cours de réplique.

2. Remplacez `us-west-2` par la région dans laquelle l'identité de domaine répliquée sera créée.
3. Remplacez `AWS_SES_US_EAST_1` par la région de signature DKIM du parent qui représente sa configuration de signature Easy DKIM qui sera répliquée sur l'identité de réplique.

 Note

Le `AWS_SES_` préfixe indique que DKIM a été configuré pour l'identité parent à l'aide d'Easy DKIM et que `US_EAST_1` c'est Région AWS là qu'il a été créé.

Vérifier la configuration de l'identité des répliques

Après avoir créé la réplique d'identité, vous pouvez vérifier qu'elle a été correctement configurée avec la configuration de signature DKIM de l'identité parent.

Pour vérifier l'identité d'une réplique :

1. Dans l' Région AWS endroit où vous avez créé la réplique d'identité, ouvrez la console SES à l'adresse <https://console.aws.amazon.com/ses/>.
2. Dans le volet de navigation, choisissez Identities et sélectionnez l'identité que vous souhaitez vérifier dans le tableau Identités.
3. Sous l'onglet Authentification, le champ de configuration DKIM indiquera le statut, et le champ Région parent indiquera la région utilisée pour la configuration de signature DKIM de l'identité à l'aide de DEED.

En utilisant AWS CLI :

Utilisez la `get-email-identity` commande spécifiant le nom de domaine et la région de la réplique :

```
aws sesv2 get-email-identity --email-identity example.com --region us-west-2
```

La réponse inclura la valeur de la région parent dans le `SigningAttributesOrigin` paramètre indiquant que l'identité de réplique a été correctement configurée avec la configuration de signature DKIM de l'identité parent :

```
{
```

```
"DkimAttributes": {  
  "SigningAttributesOrigin": "AWS_SES_US_EAST_1"  
}
```

Autorisations requises pour utiliser DEED

Pour utiliser DEED, vous devez :

1. Autorisations standard pour créer des identités e-mail dans la région de réplication.
2. Autorisation de répliquer la clé de signature DKIM depuis la région parent.

Exemple de stratégie IAM pour la réplication DKIM

La politique suivante autorise la réplication des clés de signature DKIM depuis une identité parent vers des régions de réplication spécifiées :

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AllowDKIMReplication",  
      "Effect": "Allow",  
      "Action": "ses:ReplicateEmailIdentityDKIMSigningKey",  
      "Resource": "arn:aws:ses:us-east-1:123456789124:identity/example.com",  
      "Condition": {  
        "ForAllValues:StringEquals": {  
          "ses:ReplicaRegion": ["us-east-1", "us-east-1"]  
        }  
      }  
    }  
  ]  
}
```

Bonnes pratiques

Les meilleures pratiques suivantes sont recommandées :

- Planifiez vos régions parent et de réplique : prenez en compte la région parent que vous choisissez, car elle sera la source fiable de la configuration DKIM utilisée dans les régions de réplique.
- Utilisez des politiques IAM cohérentes : assurez-vous que vos politiques IAM autorisent la réplique DKIM dans toutes les régions prévues.
- Maintenir les identités parentes actives : n'oubliez pas que vos identités de réplique héritent de la configuration de signature DKIM de l'identité parent. En raison de cette dépendance, vous ne pouvez pas supprimer d'identité parent tant que toutes les identités de réplique ne sont pas supprimées.

Résolution des problèmes

Si vous rencontrez des problèmes avec DEED, prenez en compte les points suivants :

- Erreurs de vérification : assurez-vous que vous disposez des autorisations nécessaires pour la réplique DKIM.
- Retards de réplique — Prévoyez un certain temps pour que la réplique soit terminée, en particulier lors de la création de nouvelles identités de réplique.
- Problèmes liés au DNS — Vérifiez que les enregistrements DNS de l'identité du parent sont correctement configurés et propagés.

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 moins 1024 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. Sur la ligne de commande, entrez la commande suivante pour générer la clé privée en la *nnnn* remplaçant par une longueur de bits 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'enregistre 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 enregistre texte à la configuration DNS pour votre domaine le registre doit utiliser le format suivant :

Nom	Type	Value
<i>selector</i> . _clé de domaine. <i>example.com</i>	TXT	p= <i>yourPublicKey</i>

Dans l'exemple précédent, apportez les modifications suivantes :

- *selector* Remplacez-le par un nom unique identifiant 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.
- *yourPublicKey* Remplacez-le par la clé publique que vous avez créée précédemment et incluez le p= préfixe comme indiqué dans la colonne 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.
GoDaddy	Ajout d'un registre TXT (lien externe)
DreamHost	How do I add custom DNS records? (Comment ajouter des registres DNS personnalisés ?) (lien externe)

Fournisseur DNS/d'hébergement	Lien vers la documentation
Cloudflare	Gestion des registres DNS dans CloudFlare (lien externe)
HostGator	Gérer les enregistrements DNS avec HostGator /eNom (lien externe)
Namecheap	Comment ajouter TXT/SPF/DKIM/DMARC des enregistrements 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'utiliser les AWS CLI procédures décrites dans cette section, vous devez d'abord installer et configurer le AWS CLI. Pour plus d'informations, consultez le [guide de AWS Command Line Interface l'utilisateur](#).

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 à partir du 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 :

- *example.com* Remplacez-le par le domaine que vous souhaitez créer.
- *privateKey* Remplacez-le 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.

- *selector* Remplacez-le par le sélecteur unique que vous avez spécifié lors de la création de l'enregistrement TXT dans la configuration DNS de 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 complet du 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 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 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 DomainKeys Identified Mail (DKIM), choisissez 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 Enregistrer les modifications.

Pour mettre à jour une identité de domaine à l'aide de BYODKIM à partir du 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 :

- *privateKey* Remplacez-le 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.

- *selector* Remplacez-le par le sélecteur unique que vous avez spécifié lors de la création de l'enregistrement TXT dans la configuration DNS de 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 :

- *path/to/update-identity.json* Remplacez-le par le chemin complet du fichier que vous avez créé à l'étape précédente.
- *example.com* Remplacez-le 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 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 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, le champ de configuration DKIM de votre domaine affiche Successful dans le volet DomainKeysIdentified Mail (DKIM), et le champ Identity status affiche Vérifié dans le volet Résumé.

Pour vérifier l'état DKIM d'un domaine à l'aide du AWS CLI

Après avoir configuré un domaine pour utiliser BYODKIM, vous pouvez utiliser l'GetEmailIdentityopération 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 du paramètre `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.

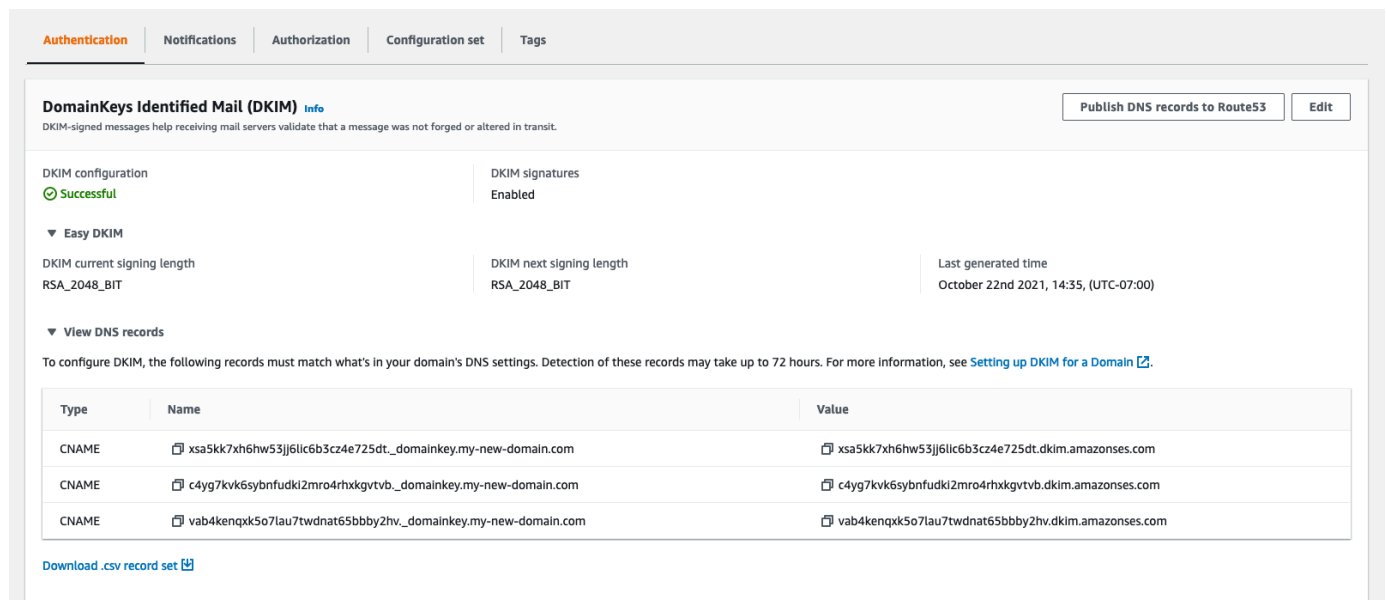
Obtention des registres DKIM pour une identité

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 des enregistrements 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": [
        "hirjd4exempld5477y22yd23ettobi",
        "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 reçu lorsque vous avez exécuté la `get-identity-dkim-attributes` commande, 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 :

```
hirjd4exempld5477y22yd23ettobi._domainkey.example.com CNAME
hirjd4exempld5477y22yd23ettobi.dkim.amazonses.com
```

```
v3rnz522czcl46quexamplek3efo5o6x._domainkey.example.com CNAME
v3rnz522czcl46quexamplek3efo5o6x.dkim.amazonses.com
y4examplexbhyhnsjcmtvzotfvqjmdqoj._domainkey.example.com CNAME
y4examplexbhyhnsjcmtvzotfvqjmdqoj.dkim.amazonses.com
```

Note

Tous n' Régions AWS utilisent pas le domaine DKIM SES par défaut.
dkim.amazonses.com Pour voir si votre région utilise un domaine DKIM spécifique à une région, consultez le tableau des [domaines DKIM](#) 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 (Identities 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 signer disable/enable DKIM pour les identités d'adresses 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.

Vers la signature disable/enable DKIM pour l'identité d'une 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 (Authentication) 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.

À la signature disable/enable DKIM pour l'identité d'une adresse e-mail à l'aide du 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. *marketing@example.com* Remplacez-le par l'identité de l'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. Après avoir créé le message et la signature DKIM, vous pouvez utiliser l'[SendRawEmail](#) API 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 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 répondre 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.

Consultez [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 [SetIdentityMailFromDomainAPI](#).

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 volet Custom MAIL FROM domain, choisissez 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	Value
<i>subdomain</i> . <i>domain.com</i>	MX	10 feedback-smtp. <i>region</i> .amazonse s.com

Nom	Type	Value
<i>subdomain .domain.com</i>	TXT	"v=spf1 include:amazonses.com ~all"

Dans les enregistrements précédents,

- *subdomain .domain.com* sera renseigné avec votre sous-domaine MAIL FROM
- *region* sera renseigné avec le nom de l' Région AWS endroit où vous souhaitez vérifier le domaine MAIL FROM (tel que `us-west-2`, `us-east-1`, `eu-west-1`, ou, 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 du SPF doit généralement inclure les guillemets, mais certains fournisseurs DNS n'en ont pas besoin.

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

- Les procédures spécifiques de publication des enregistrements MX et SPF (type TXT) dépendent de votre DNS ou de votre fournisseur d'hébergement. Consultez la documentation de votre fournisseur ou contactez-le pour obtenir des informations sur l'ajout de ces enregistrements à la configuration DNS de votre domaine.
- 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)

Nom du fournisseur DNS/d'hébergement	Lien vers la documentation
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 ajouter TXT/SPF/DKIM/DMARC des enregistrements 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	Value
<i>subdomain .domain.com</i>	MX	10 feedback-smtp. <i>region</i> .amazonse s.com
<i>subdomain .domain.com</i>	TXT	"v=spf1 include:amazonses. com ~all"

Dans les enregistrements précédents,

- *subdomain .domain .com* sera renseigné avec votre sous-domaine MAIL FROM
- *region* sera renseigné avec le nom de l' Région AWS endroit où vous souhaitez vérifier le domaine MAIL FROM (tel que us-west-2, us-east-1, eu-west-1, ou, 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)

Nom du fournisseur DNS/d'hébergement	Lien vers la documentation
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 ajouter TXT/SPF/DKIM/DMARC des enregistrements 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.

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.

State	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 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,

State	Comportement d'envoi d'e-mails	Actions Amazon SES
		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 suivante [the 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	Value
<code>_dmarc.example.com</code>	TXT	<code>"v=DMARC1;p=quarantine;rua=mailto:my</code>

Nom	Type	Value
		<code>_dmarc_report@example.com"</code>

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, voir [the 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 quarantaine `p=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 rejeter `p=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 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 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](#).

Alors que le BIMi nécessite le DMARC, le DMARC exige que votre domaine comporte des enregistrements SPF ou DKIM pour s'aligner, mais il est préférable d'inclure à la fois des enregistrements SPF et DKIM pour plus de sécurité, et parce que certains fournisseurs de services de messagerie () ESPs exigent les deux lorsqu'ils utilisent BIMi. La section suivante passe en revue les étapes d'implémentation de BIMi dans Amazon SES.

Configuration de BIMl dans SES

Vous pouvez configurer BIMl 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 BIMl dans les [clients de messagerie qui prennent en charge BIMl](#).

Avant de pouvoir afficher un logo BIMl 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 BIMl et les éléments nécessaires à sa configuration dans SES sont détaillés ici.

Pour configurer BIMl 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 BIMl, 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 spécificités de politique d'application suivantes requises pour le BIMl, comme dans l'un des deux exemples :

Nom	Type	Valeur
<code>_dmarc.example.com</code>	TXT	<code>v=DMARC1;p=quarantine;pct=100;rua=mailto:dmarcreports@example.com</code>
<code>_dmarc.example.com</code>	TXT	<code>v=DMARC1;p=reject;rua=mailto:dmarcreports@example.com</code>

Dans l'exemple de politique DMARC précédent, comme l'exige BIMl :

- *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, BIMl 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 BIMl.
 - 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 BIMl, comme indiqué.
4. Produisez votre logo BIMl sous forme de .svg fichier SVG (Scalable Vector Graphics). Le profil SVG spécifique requis par BIMl est défini comme SVG (Portable/Secure SVG P/S). Pour que votre logo s'affiche dans le client de messagerie, il doit être parfaitement conforme à ces spécifications. Reportez-vous aux conseils de [BIMl 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 ESPs, tels que Gmail et Apple, exigent qu'une VMC prouve que vous êtes propriétaire de la marque et du contenu de votre logo BIMl. Même s'il ne s'agit pas d'une condition absolue pour implémenter BIMl sur votre domaine, si l'ESP auquel vous envoyez des e-mails applique la conformité VMC, votre logo BIMl ne s'affichera pas dans le client de messagerie. Consultez les informations de référence de BIMl 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 BIMl 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 BIMl qui comporte l'URL de votre logo. Lors de la vérification de votre enregistrement DMARC, un [ESP qui prendre en charge BIMl](#) recherchera également un enregistrement BIMl 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 BIMl s'affichera.

Configurez votre domaine avec BIMl 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 avoir un modèle d'envoi régulier ESPs qui supporte le placement du logo BIMI. Votre domaine doit avoir une cadence de livraison régulière et doit avoir une bonne réputation auprès du ESPs destinataire. Le placement du logo BIMI peut prendre du temps à s'afficher ESPs là où vous n'avez pas une réputation établie ou une cadence d'envoi.

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 des notifications pour les e-mails envoyés depuis cette identité, et uniquement dans la AWS région 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 activez 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](#)
- [Désactivation du transfert de commentaires par e-mail](#)

- [Destination du transfert de commentaires par e-mail](#)

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 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 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 [SetIdentityFeedbackForwardingEnabled](#) API.

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 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 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 [SetIdentityFeedbackForwardingEnabled](#) API.

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 [JSON \(JavaScript Object Notation\)](#), 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](#)
- [Contenu des notifications Amazon SNS pour Amazon SES](#)
- [Exemples de notification Amazon SNS pour Amazon SES](#)

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 :

- [Conditions préalables](#)
- [Configuration de notifications à l'aide de la console Amazon SES](#)
- [Configuration de notifications à l'aide de l'API Amazon SES](#)
- [Dépannage des notifications de commentaire](#)

Conditions préalables

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 :

JSON

```
{
  "Version": "2012-10-17",
  "Id": "notification-policy",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ses.amazonaws.com"
      },
      "Action": "sns:Publish",
      "Resource": "arn:aws:sns:us-east-1:111122223333: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 :

- *topic_region* Remplacez-le par la AWS région dans laquelle vous avez créé le sujet SNS.
 - Remplacez *111122223333* par votre ID de compte AWS .
 - *topic_name* Remplacez-le par le nom de votre rubrique SNS.
 - Remplacez *identity_name* par l'identité vérifiée (adresse e-mail ou domaine) à laquelle vous êtes abonné 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 politique clé. AWS KMS Vous pouvez ajouter des autorisations en joignant la politique suivante à la politique AWS KMS clé :

JSON

```
{
  "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 volet de navigation, sous Configuration, choisissez Identities.
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 rebond, de réclamation et de livraison doivent être identiques à celles dans Région AWS lesquelles vous utilisez 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. Sélectionnez 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 sont au format JSON (JavaScriptObject Notation) 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 sur votre rubrique Amazon SNS échoue parce que la rubrique a été supprimée ou que vous Compte AWS n'êtes plus autorisé à publier sur cette rubrique, Amazon SES supprime la configuration de cette rubrique si elle a été configurée pour les rebonds ou les réclamations (et non pour les livraisons. Pour les notifications de livraison, SES ne supprimera pas le paramètre de configuration de la 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 politique de la AWS KMS clé. Consultez [Conditions préalables](#) pour obtenir un exemple de stratégie.

Contenu des notifications Amazon SNS pour Amazon SES

Les notifications de rebond, de réclamation et de livraison 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 :

- [Top-level Objet JSON](#)
- [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 capable d'analyser la notification Amazon SNS et de gérer les deux cas ; SES ne garantit pas les commandes ou les lots 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.
- 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.
- 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`.

Top-Level Objet JSON

L'objet JSON de niveau supérieur d'une notification 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
<code>timestamp</code>	Heure à laquelle le message a été envoyé (au format ISO8601).
<code>messageId</code>	Identifiant unique attribué par SES au message. SES vous a renvoyé cette valeur lorsque vous avez envoyé le message.  Note Cet identifiant de message a été attribué par SES. Vous trouverez l'ID de message de l'e-mail d'origine dans le champ <code>headers</code> de l'objet <code>mail</code>.
<code>source</code>	Adresse e-mail à partir de laquelle l'e-mail d'origine a été envoyé (adresse MAIL FROM de l'enveloppe).
<code>sourceArn</code>	ARN (Amazon Resource Name) de l'identité qui a été utilisée pour envoyer l'e-mail. Dans le cas d'une autorisation d'envoi, <code>sourceArn</code> 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 .
<code>sourceIp</code>	Adresse IP publique d'origine du client qui a effectué la demande d'envoi d'e-mail à SES.

Nom de champ	Description
<code>sendingAccountId</code>	L'ID du compte AWS du compte qui a été utilisé pour envoyer l'e-mail. Dans le cas de l'autorisation d'envoi, <code>sendingAccountId</code> correspond à l'ID de compte de l'expéditeur délégué.
<code>callerIdentity</code>	L'identité IAM de l'utilisateur SES qui a envoyé l'e-mail.
<code>destination</code>	Liste des adresses e-mail destinataires de l'e-mail original.
<code>headersTruncated</code>	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. SES tronque les en-têtes de la notification lorsque les en-têtes du message d'origine ont une taille supérieure ou égale à 10 Ko. Les valeurs possibles sont <code>true</code> et <code>false</code>.

Nom de champ	Description
<code>headers</code>	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 <code>name</code> et un champ <code>value</code>.  Note Tout identifiant de message contenu dans l'<code>headersobjet</code> provient du message d'origine que vous avez transmis à SES. L'ID du message que SES a ensuite attribué au message se trouve dans le <code>messageId</code> champ de l'<code>mailobjet</code>.

Nom de champ	Description
<code>commonHeaders</code>	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 <code>commonHeaders</code> correspond à l'ID de message qu'Amazon SES a par la suite affecté au message dans le champ <code>messageId</code> 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-0000000",
  "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 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	Le type de rebond, tel que déterminé par SES. Pour de plus amples informations, veuillez consulter Types de retour à l'expéditeur .
bounceSubType	Sous-type du rebond, tel que déterminé par SES. Pour de plus amples informations, veuillez consulter 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'expéditeur a été envoyé (au format ISO8601). Notez qu'il s'agit de l'heure à laquelle la notification a été envoyée par le fournisseur de services Internet, et non de l'heure à laquelle elle a été reçue par SES.
feedbackId	ID unique du retour à l'expéditeur.

Si SES a pu contacter l'autorité de transfert de messages (MTA) distante, le champ suivant est également présent.

Nom de champ	Description
<code>remoteMtaIp</code>	Adresse IP du MTA auquel SES a tenté d'envoyer 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
<code>reportingMTA</code>	Valeur du champ <code>Reporting-MTA</code> 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
<code>emailAddress</code>	Adresse e-mail du destinataire. Si un DSN est disponible, l'adresse correspond à la valeur du champ <code>Final-Recipient</code> 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
<code>action</code>	Valeur du champ <code>Action</code> du DSN. Cela indique l'action effectuée par le Reporting-MTA suite de sa tentative de remise du message à ce destinataire.
<code>status</code>	Valeur du champ <code>Status</code> du DSN. Il s'agit du code de statut indépendant du transport par destinataire qui indique le statut de remise du message.
<code>diagnosticCode</code>	Code de statut émis par la MTA de suivi. Il s'agit de la valeur du champ <code>Diagnostic-Code</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 rebond contient un type de Undetermined rebond Permanent (dur) ou Transient (doux). Les types de rebond Permanent *Transient*(dur) et (doux) peuvent également contenir l'un des nombreux sous-types de rebond.

Lorsque vous recevez une notification de rebond avec un type de rebond Transient (souple), vous pourrez peut-être envoyer un e-mail à ce destinataire à l'avenir si le problème à l'origine du rebond du message est résolu.

Lorsque vous recevez une notification de rebond avec un type de rebond Permanent (dur), il est peu probable que vous puissiez envoyer un e-mail à ce destinataire à l'avenir. 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 soft bounce (un rebond lié à un problème temporaire, tel que la boîte de réception du destinataire est pleine) se produit, SES tente de redistribuer l'e-mail pendant un certain temps. À la fin de cette période, si SES ne parvient toujours pas à délivrer l'e-mail, il arrête d'essayer.

SES fournit des notifications pour les rebonds durs et pour les rebonds souples qu'il a cessé d'essayer de délivrer. 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	rebondir SubType	Description
Undetermined	Undetermined	Le fournisseur de messagerie du destinataire a envoyé un message de retour à l'expéditeur. Le message de rebond ne contenait pas suffisamment d'informations pour que SES puisse déterminer la raison du rebond. L'e-

bounceType	rebondir SubType	Description
		mail de rebond, qui a été envoyé à l'adresse figurant dans l' Return-Path en-tête de l'e-mail à l'origine du rebond, peut contenir des informations supplémentaires sur le problème à l'origine du rebond de l'e-mail.
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'expéditeur, 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 réputation 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	rebondir SubType	Description
Permanent	Suppressed	L'adresse e-mail du destinataire figure sur la liste de suppression de SES car elle a récemment produit des hard bounces. Pour remplacer la liste de suppression globale, consultez Utilisation de la liste de suppression au niveau du compte Amazon SES .
Permanent	OnAccountSuppressionList	SES a supprimé l'envoi à cette adresse car celle-ci figure sur 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.
Permanent	OnTenantSuppressionList	SES a supprimé l'envoi à cette adresse car celle-ci figure sur la liste de suppression au niveau du locataire . Cela n'est pas pris en compte dans votre métrique de taux de retours à l'expéditeur.

bounceType	rebondir SubType	Description
Permanent	UnsubscribedRecipient	Ce type de rebond se produit lorsque le contact destinataire s'est désinscrit du sujet et qu'un e-mail lui est envoyé à l'aide des options de gestion de liste. SES respecte les préférences de contact et ne tente pas de livrer. De plus, ce rebond n'a aucun impact sur la réputation de l'expéditeur puisque la livraison n'a pas été tentée et que le contact du destinataire n'est pas ajouté à une liste de suppression en raison du rebond.  Tip Il est recommandé de vous abonner aux UnsubscribedRecipient événements pour éviter de continuer à envoyer des messages à des destinataires non abonnés. Tenez compte the section called “Utilisation de la gestion des listes”. La gestion des listes doit être la source de vérité de votre liste d'abonnés. Du point de vue de l'application du SES, si vous continuez à envoyer à des destinataires supprimés ou désabonnés, vous aurez la réputation de ne pas respecter les meilleures pratiques en matière d'envoi d'e-mails.
Permanent	EmailValidationSuppressed	SES a supprimé l'envoi à cette adresse car celle-ci n'atteignait pas le seuil de vos paramètres de validation des e-mails.

bounceType	rebondir SubType	Description
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 est de type notificationBounce, SES ne prend pas en compte les réponses automatiques lorsqu'il calcule le taux de rebond de votre compte.
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.

bounceType	rebondir SubType	Description
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. La date et l'heure indiquées dans ce champ peuvent être

Nom de champ	Description
	différentes de la date et de l'heure auxquelles 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 positiveOnAccountSuppressionList , SES a accepté le message, mais n'a pas tenté de l'envoyer car il figurait sur la liste de suppression au niveau du compte . La valeur peut également être OnTenantSuppressionList si l'adresse figurait sur la liste de suppression au niveau du locataire .

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). 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 a soumis la plainte, 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. SES effectue une recherche par rapport au message d'origine pour déterminer cette liste de destinataires.

Les objets JSON de cette liste contiennent le champ suivant.

Nom de champ	Description
<code>emailAddress</code>	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 \(Internet Assigned Numbers\)](https://www.iana.org/domains/reserved) :

- `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
<code>timestamp</code>	Heure à laquelle SES a envoyé l'e-mail au serveur de messagerie du destinataire (au format ISO8601).
<code>processingTimeMillis</code>	Le délai en millisecondes entre le moment où SES a accepté la demande de l'expéditeur

Nom de champ	Description
	et la transmission du message au serveur de messagerie du destinataire.
recipients	Liste des destinataires prévus de l'e-mail auxquels la notification de remise s'applique.
smtpResponse	Le message de réponse SMTP du fournisseur de services Internet distant qui a accepté l'e-mail de SES. Ce message varie selon l'e-mail, le serveur de messagerie de réception et l'ISP de réception.
reportingMTA	Le nom d'hôte du serveur de messagerie SES qui a envoyé le message.
remoteMtaIp	Adresse IP du MTA auquel SES a envoyé 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](#)
- [Création d'une stratégie d'autorisation d'identité dans Amazon SES](#)
- [Exemples de politiques d'identité dans Amazon SES](#)
- [Gestion de vos stratégies d'autorisation d'identité dans Amazon SES](#)

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 à l'ID de AWS compte 123456789012 les autorisations spécifiées dans la section Action pour le domaine vérifié exemple.com.

JSON

```
{
  "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.

Nom	Description	Obligatoire	Valeurs valides
<code>Id</code>	Identifie la stratégie de façon unique.	Non	Toute chaîne
<code>Version</code>	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.

Nom	Description	Obligatoire	Valeurs valides
<code>Sid</code>	Identifie l'instruction de façon unique.	Non	Toute chaîne.

Nom	Description	Obligatoire	Valeurs valides
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.

Nom	Description	Obligatoire	Valeurs valides
Principal	Spécifie Compte AWS l'utilisateur ou le AWS service qui reçoit l'autorisation dans l'instruction.	Oui	Un Compte AWS identifiant, un ARN utilisateur ou un AWS service valide. Compte AWS IDs et l'utilisateur ARNs sont spécifiés à l'aide de "AWS" (par exemple, "AWS": ["123456789012"] ou "AWS": ["arn:aws:iam::123456789012:root"]). AWS les noms de service sont spécifiés à l'aide de "Service" (par exemple, "Service": ["cognito-idp.amazonaws.com"]). Pour des exemples de format utilisateur ARNs, consultez le Références générales AWS.

Nom	Description	Obligatoire	Valeurs valides
Action	Indique l'action à laquelle s'applique l'instruction.	Oui	« ses : BatchGetMetricData », « ses : CancelExportJob », « ses : CreateDeliverabilityTestReport », CreateEmailIdentityPolicy « ses : », CreateExportJob « ses : », DeleteEmailIdentity « ses : », DeleteEmailIdentityPolicy « ses : », « ses : GetDomainStatisticsReport », GetEmailIdentity « ses : », « ses : GetEmailIdentityPolicies », « ses : GetExportJob « ses : ListExportJobs « ses : », « ses : ListRecommendations », « ses : PutEmailIdentityConfigurationSetAttributes « ses : PutEmailIdentityDomainAttributes », « ses : PutEmailIdentityDomainSigningAttributes », « ses : PutEmailIdentityFeedbackAttributes « ses : PutEmailIdentityMailFromAttributes »,

Nom	Description	Obligatoire	Valeurs valides
			« ses : TagResource « « ses : UntagResource », « ses : UpdateEmailIdentityPolicy » (Envoi d'actions d'autorisation : SendEmail « ses : », « 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 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](#).

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 politique personnalisée : si vous souhaitez inclure des conditions plus avancées ou utiliser un AWS service comme principal, vous pouvez créer une politique personnalisée et l'associer à l'identité à l'aide de la console SES ou de l'API SES.

Rubriques

- [Utilisation du Générateur de stratégies](#)
- [Création d'une stratégie personnalisée](#)

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 console Amazon SES AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/ses/>.
2. Dans le volet de navigation, sous Configuration, choisissez Identities.
3. Dans le conteneur Identités de l'écran Identités, sélectionnez l'identité vérifiée pour laquelle vous souhaitez créer une politique 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 Principaux, entrez l'Compte AWS ID, l'ARN de l'utilisateur IAM ou le AWS service pour recevoir les autorisations que vous souhaitez autoriser pour cette identité, puis choisissez 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 console Amazon SES AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/ses/>.
2. Dans le volet de navigation, sous Configuration, choisissez Identities.
3. Dans le conteneur Identités de l'écran Identités, sélectionnez l'identité vérifiée pour laquelle vous souhaitez créer une politique 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, qui est l'entité à laquelle vous accordez l'autorisation Compte AWS, peut être un utilisateur Gestion des identités et des accès AWS (IAM) ou un AWS service appartenant au même compte.

L'exemple suivant montre une politique simple qui permet à l' AWS ID 123456789012 de contrôler l'identité vérifiée exemple.com, qui appartient également à 123456789012. Compte AWS

JSON

```
{
  "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).

JSON

```
{
  "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.

JSON

```
{
  "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`.

JSON

```
{
  "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 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 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 politiques associées à une identité à l'aide de l'[opération ListIdentityPolicies d'API](#). Vous pouvez également récupérer les politiques elles-mêmes à l'aide de l'[opération GetIdentityPolicies API](#).

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 PutIdentityPolicy d'API](#).

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 DeleteIdentityPolicy API](#).

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 réclamation, de livraison et autres sur Amazon CloudWatch, Amazon Data Firehose, Amazon Pinpoint et Amazon SNS. Consultez [Créer des destination d'événement](#).
- **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](#)
- [Tâches de propriétaire d'identité pour l'autorisation d'envoi Amazon SES](#)
- [Tâches d'expéditeur délégué pour l'autorisation d'envoi Amazon SES](#)

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 [Identities vérifiées](#).
- **Expéditeur délégué** :AWS compte, utilisateur Gestion des identités et des accès AWS(IAM) ou AWS service autorisé par le biais d'une politique d'autorisation à 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.
- **Amazon Resource Name (ARN)** : méthode standardisée permettant d'identifier de manière unique une AWS ressource dans tous les AWS services. Pour l'autorisation d'envoi, la ressource est

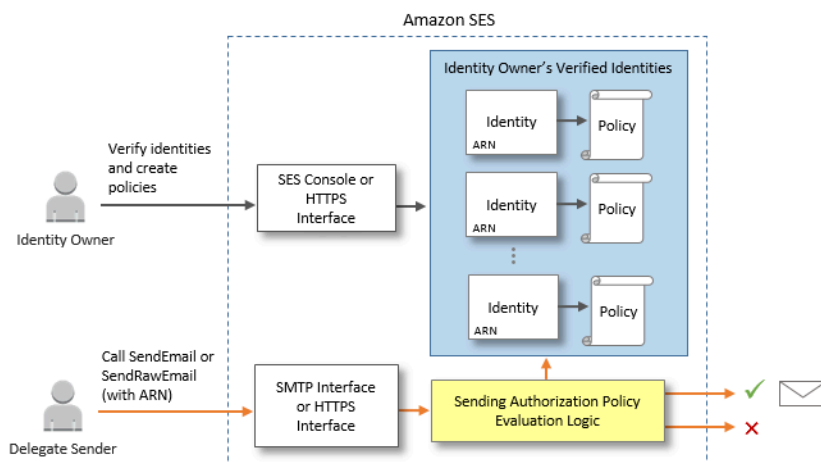
l'identité que le propriétaire de l'identité veut que l'expéditeur délégué utilise. Voici un exemple d'ARN : `arn:aws:ses:us-east-1:123456789012 : .com. identity/example`

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 [Identities verified.](#))

 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 indique au propriétaire de l'identité l'ID de AWS compte ou l'ARN de l'utilisateur IAM qu'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 de l'identité ni l'expéditeur délégué ne définissent de méthode d'envoi de notifications en cas de rebond ou de réclamation, Amazon SES envoie automatiquement des notifications d'événements par e-mail à l'adresse indiquée dans le Return-Path champ de l'e-mail (ou à l'adresse dans le champ Source, si vous n'avez pas indiqué d' Return-Path adresse), même si le propriétaire de l'identité a désactivé le transfert des 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 AWS compte de l'expéditeur délégué doit être supprimé du sandbox avant de pouvoir être utilisé pour 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 influencer sur la réputation de l'expéditeur délégué.
- Signature DKIM — Si le propriétaire de l'identité a activé la signature Easy DKIM pour une identité, tous les e-mails envoyés à partir de cette identité le seront DKIM-signed, y compris les e-mails envoyés par l'expéditeur délégué. Seul le propriétaire de l'identité peut contrôler si les e-mails le sont DKIM-signed.
- 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 [Identities 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 AWS compte de l'expéditeur délégué doit être supprimé du sandbox avant de pouvoir être utilisé pour envoyer des e-mails à des adresses non vérifiées.

- **AWS Régions** — L'expéditeur délégué doit envoyer les e-mails depuis la AWS région dans laquelle 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.
- **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](#)
- [Configuration des notifications du propriétaire d'identité pour l'autorisation d'envoi Amazon SES](#)
- [Obtention d'informations auprès de l'expéditeur délégué pour l'autorisation d'envoi Amazon SES](#)
- [Création d'une stratégie pour l'autorisation d'envoi Amazon SES](#)
- [Exemples de stratégies d'envoi](#)
- [Communication des informations d'identité à l'expéditeur délégué pour l'autorisation d'envoi Amazon SES](#)

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 [Identities vérifiées](#).

Vous pouvez confirmer qu'une adresse e-mail ou un domaine est vérifié en vérifiant son statut dans la section Identités vérifiées du <https://console.aws.amazon.com/ses/> ou en utilisant l'opération `GetIdentityVerificationAttributes` API.

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 de plus amples informations, veuillez consulter [Demande d'accès à la production \(sortie du sandbox d'Amazon SES\)](#).

 Important

- L' Compte AWS expéditeur délégué doit être supprimé du sandbox avant de pouvoir être utilisé pour envoyer des e-mails à destination ou en provenance d'adresses non vérifiées.
- Si votre compte est en sandbox, vous ne pouvez pas envoyer à des adresses e-mail qui ne sont pas vérifiées dans votre compte, même si ces domaines ou adresses e-mail ont été vérifiés dans le compte d'identité

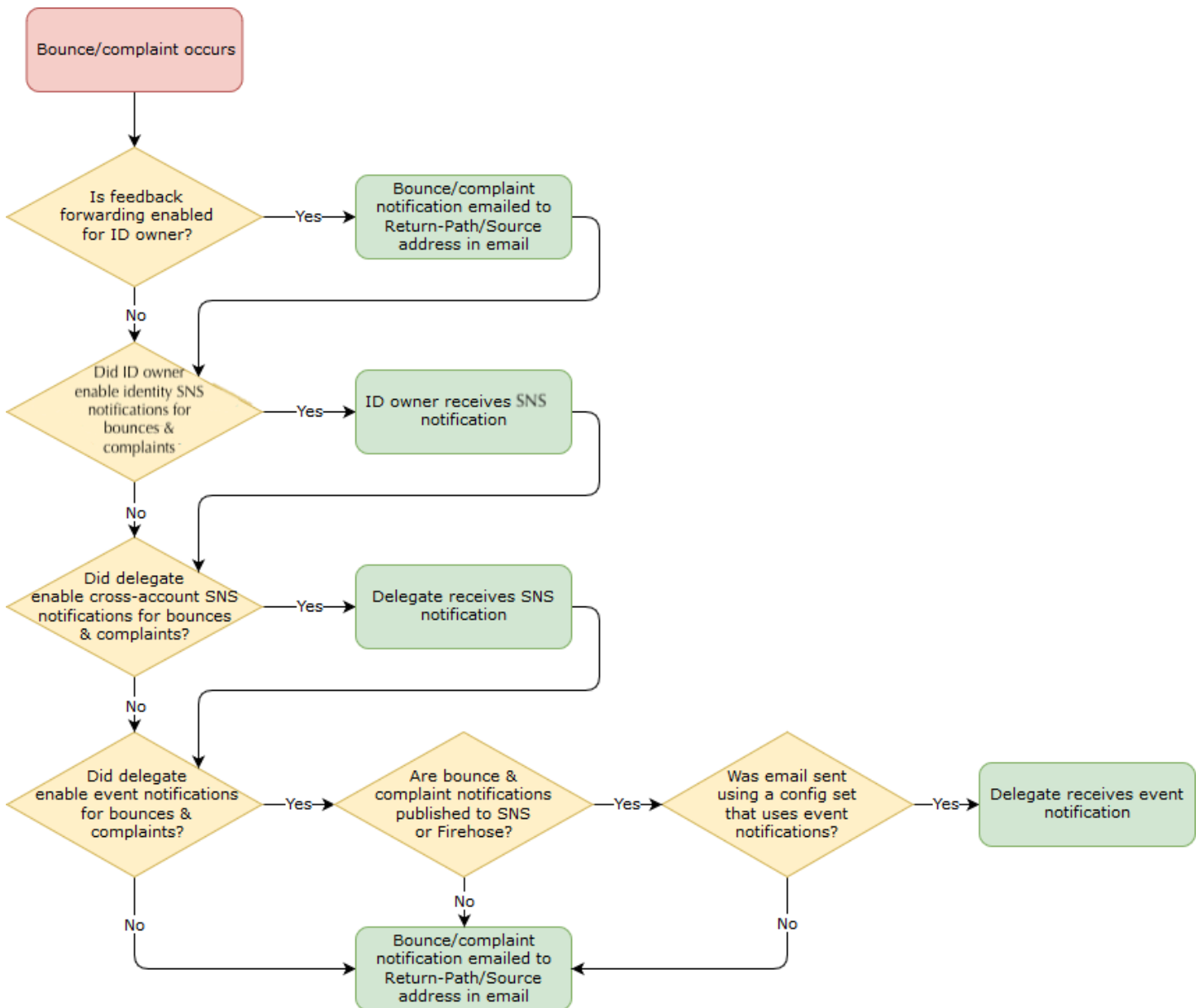
Configuration des notifications du propriétaire d'identité pour l'autorisation d'envoi Amazon SES

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 votre adresse IP apparaît sur des listes antispam tierces (DNSBL) à la suite de messages envoyés par un expéditeur délégué, la réputation de votre identité peut être entachée. DNS-based 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 de l'identité ni l'expéditeur délégué ne définissent de méthode d'envoi de notifications pour les événements de rebond et de réclamation, ou si l'expéditeur n'applique pas la configuration définie qui utilise la règle de publication des événements, Amazon SES envoie automatiquement des notifications d'événements par e-mail à l'adresse indiquée dans le Return-Path

champ de l'e-mail (ou à l'adresse dans le champ Source, si vous n'avez pas indiqué d' Return-Path adresse), même si vous avez désactivé le transfert des 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 d'Amazon SES, le principal peut être soit le AWS compte de votre expéditeur délégué, soit l'ARN de l'utilisateur Gestion des identités et des accès AWS (IAM), soit un AWS service.

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 AWS compte ou le nom de ressource Amazon (ARN) de l'utilisateur IAM afin de pouvoir 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 AWS service, consultez la documentation de ce service 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 :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSESSendEmail",
      "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](#).
- Si l'identité que vous autorisez est dupliquée dans une région secondaire dans le cadre de la fonctionnalité [Global endpoints](#), vous devrez créer des politiques d'autorisation d'envoi relatives à l'identité dans les régions principale et secondaire afin que l'expéditeur délégué soit autorisé à utiliser cette identité pour envoyer dans les deux régions.

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 console Amazon SES AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/ses/>.
2. Dans le volet de navigation, sous Configuration, choisissez Identities.
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

- vosre 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 sélectionnez Edit (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 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 console Amazon SES AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/ses/>.
2. Dans le volet de navigation, sous Configuration, choisissez Identities.
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 sélectionnez Edit (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 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 n'importe laquelle des touches AWS-wide répertoriées dans la [section Clés disponibles](#) dans le guide de l'utilisateur IAM, ou vous pouvez utiliser l'une des clés suivantes spécifiques à SES qui sont utiles pour envoyer des politiques d'autorisation :

Clé de condition	Description
<code>ses:Recipients</code>	Restreint les adresses des destinataires, qui incluent les adresses « To: », « CC » et « BCC ».
<code>ses:FromAddress</code>	Limite l'adresse d'expédition.
<code>ses:FromDisplayName</code>	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'affichage « John Doe <johndoe@example.com> » est John Doe.
<code>ses:FeedbackAddress</code>	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 principal, qui est l'entité à laquelle vous accordez l'autorisation, peut être un Compte AWS utilisateur Gestion des identités et des accès AWS (IAM) ou un AWS service.

L'exemple suivant montre une politique simple qui permet à l' AWS ID 123456789012 d'envoyer un e-mail depuis l'identité vérifiée exemple.com (qui appartient à 888888888888). Compte AWS La *Condition* déclaration contenue dans cette politique autorise uniquement le délégué (c'est-à-dire l' AWS ID 123456789012) à envoyer un e-mail à partir de l'adresse marketing+. * @example .com, où * est une chaîne que l'expéditeur souhaite ajouter après marketing+. .

JSON

```
{
```

```
"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).

JSON

```
{
  "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.

JSON

```
{
  "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' AWS organisation est spécifiée à l'aide de la clé de condition globale [PrincipalOrgID](#).

JSON

```
{
  "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-xxxxxxxxxxxx"
        }
      }
    }
  ]
}
```

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 « De », vous définissez une condition sur la clé appelée ses : FromAddress. La politique suivante permet d'envoyer l' Compte AWS ID 123456789012 à partir de l'identitéexample.com, mais uniquement à partir de l'adresse e-mail sender@example.com.

JSON

```
{
  "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.

JSON

```
{
  "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`.

JSON

```
{
  "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 politique suivante permet d'envoyer l' Compte AWS ID 123456789012 depuis `identity example.com`, mais uniquement si le nom d'affichage de l'adresse « De » inclut le marketing.

JSON

```
{
```

```
"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 déclaration autorise deux personnes Comptes AWS à envoyer depuis `sender@example.com` à condition que l'adresse « From » et l'adresse de feedback 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`.

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 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 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.

Important

Si l'identité que vous autorisez est dupliquée dans une région secondaire dans le cadre de la fonctionnalité [Global endpoints](#), remplacez le paramètre de région, tel que, par un astérisque `us-east-1`, `*` comme dans l'exemple suivant, `arn:aws:ses:*:123456789012:identity/user@example.com`

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 envoyez au nom du propriétaire de l'identité, les rebonds et les plaintes sont pris en compte dans les statistiques de rebond et de plainte de votre AWS compte, et le nombre de messages que vous envoyez est pris en compte 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 votre identifiant de AWS compte ou le nom de ressource Amazon (ARN) de votre utilisateur IAM, car vous allez envoyer un e-mail au nom du propriétaire de l'identité. Le propriétaire de l'identité a besoin des informations de votre compte afin de créer une politique vous autorisant à envoyer depuis l'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 devez partager l'ARN de votre rubrique SNS avec le propriétaire de votre identité afin qu'il puisse configurer votre rubrique SNS avec l'identité vérifiée à partir de laquelle il vous autorise à envoyer des messages.

Les procédures suivantes expliquent comment trouver les informations de votre compte et la rubrique SNS ARNs à partager avec le propriétaire de votre identité.

Pour trouver l'identifiant de votre AWS compte

1. Connectez-vous à l' AWS Management Console adresse <https://console.aws.amazon.com>.
2. Dans le coin supérieur droit de la console, augmentez votre name/account numéro et choisissez Mon compte dans le menu déroulant.
3. La page des paramètres du compte s'ouvre et affiche toutes les informations de votre compte, y compris votre identifiant de AWS compte.

Pour trouver l'ARN de votre utilisateur IAM

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à <https://console.aws.amazon.com/iam/> l'adresse.
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 l'adresse v3/home. https://console.aws.amazon.com/sns/](https://console.aws.amazon.com/sns/)

2. Dans le volet de navigation, choisissez Rubriques.
3. Dans la liste des rubriques, les rubriques SNS ARNs sont affichées 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 console Amazon SES AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/ses/>.
2. Suivez la procédure fournie dans [Créer des destination d'événement](#).
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. Consultez [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 AWS région dans laquelle le propriétaire de l'identité a vérifié l'identité.
- En outre, les AWS comptes du propriétaire de l'identité et de l'expéditeur délégué doivent être supprimés du sandbox avant que l'un ou l'autre des comptes puisse envoyer des e-mails à des adresses non vérifiées. Pour de plus amples informations, veuillez consulter [Demande d'accès à la production \(sortie du sandbox d'Amazon SES\)](#).
- Si l'identité que vous avez été autorisé à utiliser est dupliquée dans une région secondaire dans le cadre de la fonctionnalité [Global Endpoints](#) :
 - Le propriétaire de l'identité doit vous avoir fourni un ARN d'identité dont le paramètre de région, tel que `us-east-1`, a été remplacé par un astérisque, `*` comme dans l'exemple suivant, `arn:aws:ses:*:123456789012:identity/user@example.com`.
 - Le propriétaire de l'identité doit avoir créé des politiques d'autorisation d'envoi pour vous dans les régions principale et secondaire.

Utilisation de l'API Amazon SES

Comme pour tout expéditeur d'e-mail Amazon SES, si vous accédez à Amazon SES via l'API Amazon SES (soit directement via HTTPS, soit indirectement via un AWS SDK), vous pouvez choisir entre l'une des trois actions d'envoi d'e-mails suivantes : `SendEmail`, `SendTemplatedEmail` et `SendRawEmail`. Le [manuel Amazon Simple Email Service API Reference](#) en décrit les détails APIs, mais nous donnons un aperçu des paramètres d'autorisation d'envoi ici.

`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 l'adresse e-mail spécifiée dans le paramètre <code>Source</code> de <code>SendRawEmail</code> .  Note Si vous spécifiez uniquement <code>SourceArn</code> , Amazon SES définit les adresses d'expédition (<code>From</code>) et de chemin de retour (<code>ReturnPath</code> (Chemin de retour)) avec l'identité spécifiée dans <code>SourceArn</code> .
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 <code>ReturnPath</code> de <code>SendRawEmail</code> .

- 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 .
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
<code>SourceArn</code>	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 <code>Source</code> de <code>SendEmail</code> ou <code>SendTemplatedEmail</code> .
<code>ReturnPathArn</code>	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 <code>ReturnPath</code> de <code>SendEmail</code> ou <code>SendTemplatedEmail</code> .

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 console Amazon SES AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/ses/>.
2. Dans le volet de navigation, sous Configuration, sélectionnez Identités.
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 de simulateur de boîte aux lettres, vous devez l'envoyer via Amazon SES, à l' AWS CLI aide d'un AWS SDK, de la console Amazon SES, de l'interface SMTP d'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 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	bounce@simulator.amazonses.com

Scénario simulé	Adresse e-mail
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'enveloppe 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
Réclamation : le fournisseur de messagerie du destinataire accepte votre e-mail et le transmet à la boîte de réception du destinataire. Le destinataire décide que votre message est non sollicité et clique sur « Marquer comme indésirable » dans son client de messagerie. 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 commentaire de réclamation, consultez Configuration de notifications d'événement pour Amazon SES.	complaint@simulator.amazonses.com

Scénario simulé	Adresse e-mail
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 suppression 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 :

```
X50!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 envoyez 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. Consultez [Comprendre les jeux de configurations par défaut](#).

Table des matières

- [Création de jeux de configuration dans SES](#)

- [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. Informations générales — Cette section fournit des options pour personnaliser votre ensemble de configuration :
 - Nom du jeu de configuration : nom de votre jeu de configuration. Le nom peut contenir jusqu'à 64 caractères alphanumériques : les lettres, les chiffres, les tirets (-) et les traits de soulignement (_) uniquement.
 - Envoi d'un pool d'adresses IP : lorsque vous envoyez un e-mail à l'aide de cet ensemble de configuration, les messages sont envoyés à partir des adresses IP dédiées du pool attribué. 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
 - Utiliser un domaine de redirection personnalisé : cochez la case pour utiliser un domaine de redirection personnalisé afin de gérer le suivi des ouvertures et des clics pour les e-mails envoyés avec cet ensemble de configuration.
 - Domaine de redirection personnalisé : sélectionnez un domaine vérifié dans la liste Choisissez un domaine vérifié comme domaine de redirection personnalisé. Vous pouvez également saisir un sous-domaine dans le champ Entrez un sous-domaine.

 Note

Les domaines de redirection personnalisés peuvent être spécifiés comme suit :

- Vous devez d'abord créer et vérifier un domaine de redirection personnalisé dans le domaine dans lequel Région AWS vous souhaitez envoyer et suivre les e-mails, ainsi que configurer un réseau de diffusion de contenu (CDN). Ceci est expliqué dans [Configuration de domaines personnalisés pour gérer le suivi des ouvertures et des clics](#).
- Ensuite, pour utiliser votre domaine de redirection personnalisé pour le suivi des ouvertures et des clics, vous devez l'indiquer lors de la création ou de la modification de votre configuration définie ici à cette étape.
- Enfin, après avoir spécifié votre domaine de redirection personnalisé, les enregistrements View DNS apparaîtront dans le conteneur des détails généraux du jeu de configuration. Si vous le développez, vous verrez l'enregistrement CNAME contenant le domaine de suivi utilisé dans votre Région AWS. Par exemple, si votre sous-domaine personnalisé s'appelle marketing.example.com et qu'il a été créé dans les enregistrements DNS View Région AWS **Sus-east-1**, l'extension des enregistrements DNS révélera un enregistrement CNAME avec les valeurs suivantes : Name = marketing.example.com et Value = r.us-east-1.awstrack.me.

Vous pouvez utiliser ces informations simplement pour confirmer que vous avez choisi le bon domaine de suivi dans le tableau lorsque vous configurez votre CDN comme expliqué dans [Configuration de domaines personnalisés pour gérer le suivi des ouvertures et des clics](#), ou vous pouvez le faire d'abord et utiliser les valeurs d'enregistrement CNAME d'ici pour les utiliser dans votre configuration de CDN.

- Politique HTTPS — Sélectionnez une option de politique HTTPS pour le protocole des liens de suivi des ouvertures et des clics pour votre domaine de redirection personnalisé :
 - Facultatif — (Comportement par défaut) Les liens de suivi ouverts seront encapsulés à l'aide du protocole HTTP. Les liens de suivi des clics seront encapsulés selon le protocole original du lien.
 - Obligatoire — Les liens de suivi des ouvertures et des clics seront tous deux encapsulés à l'aide du protocole HTTPS.
 - Obligatoire pour les ouvertures — Les liens de suivi ouverts seront encapsulés à l'aide du protocole HTTPS. Les liens de suivi des clics seront encapsulés selon le protocole original du lien.
- Options de livraison avancées : cliquez sur la flèche de gauche pour développer la section des options de livraison avancées.
- Transport Layer Security (TLS) : 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, cochez la case 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](#).

- Durée de livraison maximale : pour spécifier le délai dans lequel SES doit tenter de livrer des e-mails via ce jeu de configuration, entrez une valeur en secondes comprise entre 300 et 50 400.

 Note

La définition d'une limite de livraison maximale personnalisée (inférieure à 14 heures par défaut de SES) peut être utile dans des cas tels que les e-mails urgents (tels que ceux contenant un mot de passe à usage unique), les e-mails transactionnels et les e-mails dont vous souhaitez vous assurer qu'ils ne sont pas livrés en dehors des heures de bureau.

 Tip

- Pour calculer les minutes en secondes, multipliez par 60, par exemple, 7 minutes* 60 = 420 secondes.

- Pour calculer les heures en secondes, multipliez par 3 600, par exemple, 2 heures* 3 600 = 7 200 secondes.

5. Options de réputation : cette section explique comment configurer les indicateurs 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](#).)
- Activé : cochez cette case pour activer les métriques de réputation pour le jeu de configuration.

6.

Options de liste de suppression : cette section fournit un ensemble de décisions permettant de définir une suppression personnalisée, en commençant par la possibilité d'utiliser cet ensemble de configuration pour annuler 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.

Options de Virtual Deliverability Manager : cette section ne sera présente que si les fonctionnalités de Virtual Deliverability Manager sont activées. Vous pouvez définir ici des paramètres personnalisés indiquant comment cet ensemble de configuration utilisera le suivi des engagements et la diffusion partagée optimisée en remplaçant la façon dont ils ont été définis dans les paramètres de votre gestionnaire de délivrabilité virtuelle au niveau du compte :

- 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. Options d'archivage — Cette section fournit la possibilité d'archiver les e-mails envoyés à partir de ce jeu de configuration :
 - a. Activez la case à cocher Enabled (Activé).
 - b. Cliquez dans le champ Archive et sélectionnez une archive dans la liste puis sur Enregistrer les modifications, ou choisissez Créer une archive et passez aux étapes restantes.
 - c. Entrez un nom unique dans le champ Nom de l'archive.
 - d. (Facultatif) Sélectionnez une période de conservation dans le champ Période de conservation pour remplacer la période de conservation par défaut de 180 jours.
 - e. (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 cléAWS KMS.
 - f. Choisissez Créer une archive.
 9. Balises — Dans cette section, vous pouvez éventuellement ajouter une ou plusieurs balises à votre ensemble de configuration :
 - 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.
10. 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. Consultez [Création de destinations d'événement Amazon SES](#).

Créez un ensemble de configuration (AWS CLI)

Vous pouvez créer un jeu de configuration à l'aide d'un fichier JSON en entrée 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",
    "HttpsPolicy": "REQUIRE"
  },
  "DeliveryOptions": {
    "TlsPolicy": "REQUIRE",
    "SendingPoolName": "sending pool",
    "MaxDeliverySeconds": 300
  },
  "ReputationOptions": {
    "ReputationMetricsEnabled": true,
    "LastFreshStart": timestamp
  },
  "SendingOptions": {
    "SendingEnabled": true
  },
  "Tags": [
    {
      "Key": "tag key",
      "Value": "tag value"
    }
  ],
  "SuppressionOptions": {
    "SuppressedReasons": ["BOUNCE", "COMPLAINT"]
  },
  "ArchivingOptions": {
```

```
"ArchiveArn": "arn:aws:ses:us-east-1:123456789012:mailmanager-  
archive/MyArchiveID"  
}  
}
```

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 un ensemble de configurations \(console\)](#)
- [Répertorier les ensembles de configuration \(AWS CLI\)](#)
- [Obtenez les détails du jeu de configuration \(AWS CLI\)](#)
- [Supprimer un ensemble de configuration \(AWS CLI\)](#)

- [Arrêter d'envoyer des e-mails à partir d'un ensemble 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 un ensemble 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. Sélectionnez un nom dans la liste des ensembles de configuration pour ouvrir sa page de détails dans l'onglet Vue d'ensemble, où vous pouvez afficher, modifier ou désactiver les options que vous avez sélectionnées. La même chose peut être faite pour les options de destination des événements en sélectionnant son onglet. Pour plus d'informations sur chaque option et ses champs, consultez la section correspondante dans [Créer un jeu de configurations \(console\)](#).
4. En haut de la page de détails de chaque ensemble de configuration, visible depuis l'onglet Vue d'ensemble ou depuis l'onglet de destination Événements, se trouvent 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.

Répertorier les ensembles de configuration (AWS CLI)

Vous pouvez utiliser la list-configuration-sets commande du 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
```

Supprimer un ensemble de configuration (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
```

Arrêter d'envoyer des e-mails à partir d'un ensemble 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 [Modifier 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 [Modifier 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'évènement.

Pour en savoir plus sur les types événement, 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 choisissez Select 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 pour 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, choisissez Add 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](#).

Modifier ou supprimer la destination d'un événement disabling/enabling

Procédez comme suit pour modifier ou supprimer une destination d'événement à l'aide de la console SES : disable/enable

Pour modifier ou supprimer une destination d'événement à l'aide de la console SES, procédez comme suit : disable/enable

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 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. `disable/enable`

Pour modifier ou supprimer une destination d'événement à l'aide de l'API SES : `disable/enable`

1. Pour disabling/enabling une destination d'événement utilisant l'API SES, consultez [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 pools d'adresses IP dédiés standard pour les serveurs dédiés IPs \(standard\)](#).
- de nouveaux groupes d'adresses IP gérées, consultez [Création d'un pool d'adresses IP géré pour activer le service dédié IPs \(géré\)](#).
- `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

- Tout `{{ses:openTracker}}` espace réservé supérieur à un sera supprimé lors de l'envoi par SES.
- N'ajoutez qu'un seul `{{ses:openTracker}}` espace réservé si vous les utilisez dans un modèle d'e-mail, car plusieurs d'entre eux entraîneront le renvoi `400 BadRequestException` d'un code d'erreur.

Pour enregistrer les clics sur les liens, SES remplace les liens contenus dans vos e-mails par des liens vers un serveur géré par SES. Cela redirige immédiatement le destinataire vers sa destination initiale. La taille totale des en-têtes, cookies compris, des requêtes adressées à ce serveur ne doit pas dépasser 8192 octets, sinon un code d'erreur `400 BadRequestException` est renvoyé.

Vous avez également la possibilité d'utiliser vos propres domaines, plutôt que des domaines détenus et exploités par SES, afin de 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 décrit les procédures de configuration d'un sous-domaine sur un serveur dont vous êtes le propriétaire afin de rediriger automatiquement les utilisateurs vers les serveurs de suivi des ouvertures et des clics exploités par 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. Consultez [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. Créez un sous-domaine à utiliser pour les liens de suivi des ouvertures et des clics. SES recommande que ce sous-domaine soit spécifiquement dédié à la gestion de ces liens et qu'un sous-domaine soit créé pour chaque e-mail que Région AWS vous envoyez et que vous souhaitez suivre.

2. Vérifiez le sous-domaine à utiliser avec SES. Pour de plus amples informations, veuillez consulter [Création d'une identité de domaine](#).
3. Ajoutez un nouvel enregistrement CNAME aux paramètres DNS de votre sous-domaine qui redirige les demandes vers le domaine de suivi SES. L'adresse vers laquelle vous redirigez doit être Région AWS identique à celle de votre sous-domaine personnalisé.
 - Utilisez le [tableau des domaines de suivi](#) dans le Références générales AWS pour sélectionner le domaine de suivi situé dans la même région que votre domaine personnalisé.

 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 également utiliser un domaine HTTPS pour suivre les clics ouverts et sur les liens. Pour configurer un domaine HTTPS afin de suivre les clics ouverts et sur les liens, vous devez effectuer certaines étapes supplémentaires, en plus de celles requises pour [configurer un domaine HTTP](#).

Pour configurer un sous-domaine HTTPS afin de gérer les liens d'ouvertures et de clics

1. Créez un sous-domaine à utiliser pour les liens de suivi des ouvertures et des clics. SES recommande que ce sous-domaine soit spécifiquement dédié à la gestion de ces liens et qu'un sous-domaine soit créé pour chaque e-mail que Région AWS vous envoyez et que vous souhaitez suivre.
2. Vérifiez le sous-domaine à utiliser avec SES. Pour de plus amples informations, veuillez consulter [Création d'une identité de domaine](#).
3. Créez un nouveau compte auprès d'un réseau de diffusion de contenu (CDN), tel qu'[Amazon CloudFront](#), voir [Commencer avec une CloudFront distribution de base](#).
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 pointer vers le domaine AWS de suivi situé dans la même région que votre domaine personnalisé. Le CDN doit transmettre l'Host en-tête fourni par le demandeur à l'origine. Consultez cet [article de AWS Re:Post](#) pour plus d'informations.

- Utilisez le [tableau des domaines de suivi](#) dans le Références générales AWS pour sélectionner le domaine de suivi situé dans la même région que votre domaine personnalisé.
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.
7. Vous pouvez utiliser la commande curl suivante pour vérifier que le domaine personnalisé que vous venez de créer utilise la région et le protocole HTTPS appropriés. Dans l'exemple suivant, tout est littéral à l'exception du nom de votre domaine :

```
curl --head https://custom.domain.com/favicon.ico
```

Une réponse est renvoyée comme dans l'exemple suivant :

```
(python-sdk-test) jdoe@12a34567b89c BaconRedirectService % curl --head https://  
custom.domain.com/favicon.ico  
HTTPS/1.1 200 OK  
x-amz-ses-region: us-east-1  
x-amz-ses-request-protocol: https  
Content-Type: image/x-icon  
Transfer-Encoding: chunked  
Date: Fri, 30 Aug 2024 13:50:14 GMT
```

Cette réponse contient les propriétés suivantes :

- La valeur `x-amz-ses-region` d'en-tête est la région SES qui a reçu la demande.
- La valeur `x-amz-ses-request-protocol` d'en-tête est le protocole utilisé pour la demande entre le CDN et SES dans l'en-tête.

Si votre configuration est correcte, la région doit refléter la région dans laquelle votre domaine a été créé et le protocole doit être HTTPS.

Partie 2 : Spécification de votre domaine de redirection personnalisé et de votre politique HTTPS via un ensemble de configuration

Après avoir configuré votre domaine pour gérer les redirections d'ouverture et de suivi des clics, vous devez spécifier votre domaine personnalisé et votre politique HTTPS dans un ensemble de configuration.

Lorsque vous envoyez un e-mail à l'aide d'un ensemble de configuration, si celui-ci est configuré pour utiliser un domaine de redirection personnalisé, les liens d'ouverture et de clic contenus dans cet e-mail utilisent automatiquement le domaine personnalisé et les options de politique HTTPS spécifiées dans le jeu de configuration.

Vous pouvez effectuer cette opération à l'aide de la console SES ou de l'opération API [CreateConfigurationSetv2](#).

Pour spécifier un domaine de redirection personnalisé et une politique HTTPS à l'aide de la console

- Lors de la création ou de la modification d'un ensemble de configuration, utilisez les [options de suivi](#) de l'étape 4 [Créer des jeux de configuration](#) pour spécifier votre domaine de redirection personnalisé et vos options de politique HTTPS.

Pour spécifier un domaine de redirection personnalisé et une politique HTTPS à l'aide du AWS CLI

Vous pouvez utiliser l'[CreateConfigurationSet](#) opération dans l'API SES v2 et utiliser la `TrackingOptions` propriété pour spécifier votre domaine de redirection personnalisé et la politique HTTPS. Vous pouvez appeler cette opération à partir du AWS CLI, comme indiqué dans l'exemple suivant.

- Créez le paramètre de configuration dans l'Région AWS endroit où vous souhaitez envoyer et suivre les e-mails :

```
aws sesv2 create-configuration-set --cli-input-json file://create.json
```

- Dans cet exemple, le fichier d'entrée utilise les paramètres de la [TrackingOptions](#) propriété : CustomRedirectDomain indique le domaine personnalisé à utiliser pour le suivi des liens ouverts et cliqués, et HttpsPolicy spécifie une option de politique HTTPS :

```
{
  "ConfigurationSetName": "my-config-set",
  "TrackingOptions": {
    "CustomRedirectDomain": "marketing.example.com",
    "HttpsPolicy": "REQUIRE"
  },
  "SendingOptions": {
    "SendingEnabled": true
  }
}
```

Pour le HttpsPolicy paramètre, les valeurs suivantes peuvent être spécifiées pour définir le protocole des liens d'ouverture et de suivi des clics pour votre domaine de redirection personnalisé :

- OPTIONAL— (Comportement par défaut) Les liens de suivi ouverts seront encapsulés à l'aide du protocole HTTP. Les liens de suivi des clics seront encapsulés selon le protocole original du lien.
- REQUIRE— Les liens de suivi des ouvertures et des clics seront tous deux encapsulés à l'aide du protocole HTTPS.
- REQUIRE_OPEN_ONLY— Les liens de suivi ouverts seront encapsulés à l'aide du protocole HTTPS. Les liens de suivi des clics seront encapsulés selon le protocole original du lien.

Partie 3 : Spécification des types d'événements d'ouverture et de clic via un ensemble de configuration

Après avoir défini votre domaine personnalisé et votre politique HTTPS dans la configuration définie à l'étape précédente, vous devez spécifier les types d'événements open and/or click à suivre dans une destination d'événement via un ensemble de configuration.

Vous pouvez effectuer cette opération à l'aide de la console SES ou de l'opération API [CreateConfigurationSetEventDestinationv2](#).

Pour sélectionner les types d'événements and/or « open click » à l'aide de la console

- Lors de la création ou de la modification d'une destination d'événement, utilisez [Ouvrir et suivre](#) les clics [the section called “Création d'une destination d'événement”](#) à l'étape 6 pour spécifier les types d'événements.

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 voir les procédures détaillées d'envoi d'e-mails qui incluent des références à des jeux de configurations, consultez les éléments suivants :

- [Envoi d'e-mails via Amazon SES à l'aide d'un AWS Kit 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 des métriques de réputation pour des jeux 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.

Utilisation de points de terminaison mondiaux dans Amazon SES

Amazon SES Global Endpoints est une fonctionnalité qui améliore la continuité et la fiabilité de vos opérations d'envoi d'e-mails. Ce chapitre vous expliquera le concept, la configuration et l'utilisation des points de terminaison mondiaux, en vous aidant à tirer parti de l'envoi multirégional (MRS) pour améliorer la disponibilité et les capacités de reprise après sinistre de vos charges de travail de messagerie.

Que sont les points de terminaison mondiaux ?

Les points de terminaison globaux sont des ressources qui vous permettent de répartir vos charges de travail sortantes SES sur deux régions AWS. Une fois configuré, SES divise automatiquement votre trafic d'envoi entre les régions principale et secondaire sélectionnées. Si l'une des régions est affectée, SES transférera automatiquement le trafic hors de la région concernée afin de maintenir la continuité de vos opérations d'envoi.

Les principaux avantages de l'utilisation de points de terminaison mondiaux sont les suivants :

- Continuité d'envoi d'e-mails améliorée
- Basculement automatique entre les régions
- Configuration multirégionale simplifiée

Comment fonctionnent les points de terminaison mondiaux

Lorsque vous configurez un point de terminaison global, vous sélectionnez une région principale (où le point de terminaison est créé) et une région secondaire. SES crée ensuite un point de terminaison multirégional (MREP) qui sert de point d'entrée pour vos demandes d'envoi d'e-mails.

Le processus de configuration globale des terminaux synchronise les principaux artefacts et les limites d'envoi de votre région principale vers votre région secondaire. Cela garantit que les deux régions ont des identités vérifiées équivalentes, des ensembles de configuration et des limites d'envoi approuvées suffisants pour l'ensemble du volume attendu.

Une fois que le point de terminaison global est prêt et que son ID de point de terminaison est spécifié dans l'appel d' `SendEmail` API, SES achemine automatiquement votre trafic sortant entre vos régions

principale et secondaire. Si l'une des régions est altérée, le trafic sera pondéré de cette région vers l'autre jusqu'à ce que le problème soit résolu.

Configuration des points de terminaison globaux

Rubriques

- [Conditions préalables](#)
- [Création d'un point de terminaison global](#)
- [États des terminaux mondiaux](#)

Conditions préalables

Avant de créer un point de terminaison global, vous devez d'abord autoriser SES à créer Service-Linked des rôles (SLR) dans votre compte. Ces rôles permettent les fonctionnalités de service essentielles et l'accès aux ressources nécessaires pour créer, utiliser et surveiller les points de terminaison mondiaux. Cela peut être fait en mettant en œuvre la politique suivante :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "ses.amazonaws.com"
        }
      }
    }
  ]
}
```

Création d'un point de terminaison global

Pour créer un nouveau point de terminaison global :

1. Ouvrez la console SES à l'adresse <https://console.aws.amazon.com/ses/>.
2. Dans le volet de navigation, sélectionnez Global Endpoints.
3. Choisissez Create global endpoint et entrez un nom dans le champ Nom.
4. Sélectionnez une région secondaire dans le menu déroulant. (Votre région principale est par défaut la région avec laquelle vous vous êtes connecté à la console.)
5. (Facultatif) Ajoutez une ou plusieurs balises à votre point de terminaison global.
6. Passez en revue la configuration et choisissez Create global endpoint.

Le processus de création peut prendre quelques secondes. Une fois terminé, le statut de votre point de terminaison global passera à « Prêt ».

En utilisant AWS CLI :

```
aws sesv2 create-multi-region-endpoint --primary-region us-west-2 --secondary-region us-east-1 --endpoint-name MyGlobalEndpoint
```

Dans l'exemple précédent :

- Remplacez *us-west-2* par la région principale de votre point de terminaison mondial.
- Remplacez *us-east-1* par la région secondaire de votre point de terminaison mondial.
- *MyGlobalEndpoint* Remplacez-le par le nom convivial à donner à votre point de terminaison global.

États des terminaux mondiaux

Les points de terminaison globaux peuvent avoir les états suivants :

- Création — La ressource est en cours de provisionnement
- Prêt — La ressource est prête à être utilisée
- Échec : la ressource n'a pas pu être provisionnée
- Suppression — La ressource est supprimée comme demandé

Préparation de la région secondaire

Maintenant que vous avez créé votre point de terminaison global, vous devez vous assurer que la configuration d'envoi de vos e-mails, y compris tous ses composants (identités, ensembles de configuration, modèles d'e-mails et limites d'envoi), est cohérente entre les régions principale et secondaire avant d'utiliser le point de terminaison global pour envoyer des e-mails. Cet alignement est essentiel pour éviter les problèmes potentiels et garantir une livraison et un suivi corrects des e-mails.

La fonctionnalité de duplication des régions de la console vous aide en dupliquant automatiquement les ressources et en dupliquant les paramètres au niveau du compte de la région principale vers la région secondaire, ce qui vous aidera rapidement à vous assurer que les deux régions ont des configurations équivalentes.

En fonction des dépendances des ressources, l'ordre dans lequel vous dupliquez les ressources est important. Pour éviter les conflits, suivez l'ordre des sujets ci-dessous :

Rubriques

- [Duplication d'ensembles de configuration](#)
- [Duplication des identités de domaine vérifiées](#)
- [Duplication des limites de production](#)

Duplication d'ensembles de configuration

Vous pouvez sélectionner plusieurs ensembles de configuration de votre région principale à dupliquer, ainsi que leurs paramètres, dans la région secondaire.

La fonctionnalité « Dupliquer les ensembles de configuration » vous permet de :

- Dupliquez simultanément plusieurs ensembles de configuration dans la région secondaire.
- Vérifiez les différences entre les ensembles de configuration de la région principale et de la région secondaire.

Pour dupliquer des ensembles de configuration :

1. Sur la page Points de terminaison globaux, choisissez le point de terminaison global que vous souhaitez dupliquer en le sélectionnant dans la colonne Nom.

2. Dans la carte Dupliquer les ensembles de configuration, développez les actions des ensembles de configuration et choisissez Dupliquer.
3. Sélectionnez jusqu'à 10 ensembles de configuration, puis cliquez sur Confirmer.
4. Si le statut n'est pas satisfaisant, choisissez Afficher le rapport pour identifier le problème.
5. (Facultatif) Pour les ensembles de configuration précédemment dupliqués, vous pouvez vérifier les différences entre les régions principale et secondaire en sélectionnant Vérifier les différences tout en répétant les trois dernières étapes.

Note

- Si le jeu de configuration que vous avez dupliqué contient des destinations d'événements, des options de réputation, des options d'archivage, ou s'il est référencé dans un modèle d'e-mail, ces paramètres devront être configurés manuellement dans la région secondaire.
- Si l'archivage des e-mails envoyés (sortants) est activé dans une configuration définie dans la région principale, vous devez activer manuellement l'archivage des e-mails envoyés (sortants) dans le jeu de configuration de la région secondaire à l'aide d'une archive créée dans la région secondaire avec le même nom.

Duplication des identités de domaine vérifiées

Pour garantir le bon fonctionnement de la configuration globale du point de terminaison, l'identité de votre domaine d'envoi doit être vérifiée dans les régions principale et secondaire. SES s'[DKIM facile déterministe \(DEED\)](#) en sert pour simplifier ce processus.

[Deterministic Easy DKIM \(DEED\)](#) est une fonctionnalité qui génère des jetons DKIM cohérents dans tous les domaines sur la Région AWS base d'un domaine parent configuré avec Easy DKIM. Cette cohérence permet à SES de vérifier automatiquement un domaine dans la région secondaire une fois qu'il est vérifié dans la région principale, sans nécessiter de mises à jour supplémentaires des enregistrements DNS. Par conséquent, vous devez vous assurer que l'identité de domaine que vous souhaitez dupliquer, c'est-à-dire le parent, est déjà configurée avec Easy DKIM.

La fonctionnalité « Identités de domaine vérifiées dupliquées » vous permet de :

- Dupliquez simultanément plusieurs identités de domaine dans la région secondaire.
- Vérifiez-les automatiquement avec Deterministic Easy DKIM (DEED).

- Vérifiez les différences entre les identités de la région principale et de la région secondaire.

Pour dupliquer des identités depuis la console SES :

1. Sur la page Points de terminaison globaux, choisissez le point de terminaison global que vous souhaitez dupliquer en le sélectionnant dans la colonne Nom.
2. Dans la carte Identités de domaine vérifiées dupliquées, développez les actions Identités et choisissez Dupliquer.
3. Sélectionnez jusqu'à 10 identités, puis cliquez sur Confirmer.
4. Si le statut n'est pas satisfaisant, choisissez Afficher le rapport pour identifier le problème.
5. (Facultatif) Pour les identités précédemment dupliquées, vous pouvez vérifier les différences entre les régions principale et secondaire en sélectionnant Vérifier les différences tout en répétant les trois dernières étapes.

Note

- Les identités de domaine vérifiées avec BYODKIM, ou auto-signées, devront être créées manuellement dans la région secondaire, car le DEED n'est pas applicable dans ce cas.
- Les identités de domaine utilisant des Mail-from attributs, des politiques ou le transfert de commentaires et les notifications devront être configurées manuellement dans la région secondaire.

Duplication des limites de production

SES vérifie si les limites d'envoi sont alignées entre les régions et vous permet de demander des augmentations de limites dans la région secondaire si nécessaire.

La fonctionnalité « Limites de production dupliquées » vous permet de :

- Vérifiez si les limites de production sont alignées entre les régions principales et secondaires.
- Demandez une augmentation de limite dans la région secondaire si nécessaire.

Pour dupliquer les limites de production :

1. Sur la page Points de terminaison globaux, choisissez le point de terminaison global que vous souhaitez dupliquer en le sélectionnant dans la colonne Nom.
2. Dans la carte Limites de production dupliquées, si le statut indique Limites d'envoi non alignées, développez les actions relatives aux limites d'envoi.
3. Sélectionnez Gérer les limites d'envoi pour la région secondaire.
4. La page Quotas de Service s'ouvre dans la région secondaire où vous pouvez demander l'augmentation du « Quota d'envoi » et du « Taux d'envoi » afin de correspondre aux valeurs de la région principale.

 Tip

Il est recommandé de demander le quota maximum auquel vous êtes éligible dans les deux régions. Bien que le trafic de courrier électronique soit réparti entre les deux régions dans des conditions de fonctionnement normales, lors d'un incident de basculement, le volume total du trafic de courrier électronique sera envoyé vers une région et ses limites devraient être suffisantes pour gérer la charge totale du volume.

5. (Facultatif) Vous pouvez également demander des augmentations de production pour votre région principale en sélectionnant Gérer les limites d'envoi pour la région principale tout en répétant les deux étapes précédentes.

 Important

Il est essentiel que les deux régions disposent des identités vérifiées et des ensembles de configuration équivalents avec lesquels vous avez l'intention d'envoyer des e-mails, ainsi que des limites d'envoi correspondantes pour garantir le bon fonctionnement du point de terminaison mondial. Toute anomalie peut entraîner des échecs de livraison, une diminution de la fiabilité du basculement et des indicateurs manquants.

Utilisation de points de terminaison globaux

Rubriques

- [Intégration à votre application](#)

- [Surveillance et mesures](#)

Intégration à votre application

L'utilisation d'un point de terminaison global dans votre application nécessite que vous obteniez son identifiant de point de terminaison.

Pour récupérer l'ID de point de terminaison global d'un point de terminaison :

1. Depuis la console SES, accédez à la page des points de terminaison globaux et choisissez le point de terminaison global que vous souhaitez utiliser en le sélectionnant dans la colonne Nom.
2. Sélectionnez l'icône de copie sous ID du point de terminaison sur la page des détails du point de terminaison global.

En utilisant AWS CLI :

```
aws sesv2 get-multi-region-endpoint --endpoint-name MyGlobalEndpoint --region us-west-2
```

Dans l'exemple précédent :

- *MyGlobalEndpoint* Remplacez-le par le nom convivial que vous avez donné à votre point de terminaison global lors de sa création.
- Remplacez *us-west-2* par la région principale dans laquelle vous avez créé votre point de terminaison global.
- La réponse de l'API inclura la valeur de votre identifiant de point de terminaison, par exemple, "EndpointId": "abcdef12.g3h".

Une fois que vous avez obtenu l'identifiant de point de terminaison de votre point de terminaison global, vous pouvez mettre à jour vos appels [SendEmail](#) ou vos appels d'[SendBulkEmail](#) API pour inclure la valeur de l'identifiant de point de terminaison pour le `endpoint-id` paramètre. Voici un exemple de la manière de spécifier l'identifiant du point de terminaison dans un appel d' `SendEmail` API à l'aide de AWS CLI :

```
aws sesv2 send-email \  
    --from-email-address "sender@example.com" \  
    --destination "ToAddresses=recipient@example.com" \  
    --endpoint-id "abcdef12.g3h"
```

```
--content "Subject={Data=Test
email,Charset=UTF-8},Body={Text={Data=This is a test email sent using Amazon SES
Global endpoints.,Charset=UTF-8}}" \
--endpoint-id "abcdef12.g3h"
```

abcdef12.g3h Remplacez-le par l'identifiant du point de terminaison réel que vous avez obtenu via la console ou l'API.

Surveillance et mesures

La fonctionnalité Global Endpoints fournit une vue unifiée de votre volume d'envoi d'e-mails dans les régions principale et secondaire. Vous pouvez accéder à ces métriques via l'onglet Cross-region Metrics sur la page des détails du point de terminaison global de la console SES.

Pour accéder aux statistiques d'envoi dans les deux régions :

1. Depuis la console SES, accédez à la page Points de terminaison globaux, choisissez le point de terminaison global pour lequel vous souhaitez voir les métriques en le sélectionnant dans la colonne Nom.
2. Sélectionnez l'onglet Cross-region Mesures sur la page des détails du point de terminaison global et entrez une plage de dates allant jusqu'à 31 jours. Les statistiques des deux régions seront affichées pour la plage de dates donnée.

En utilisant AWS CLI :

```
aws cloudwatch get-metric-statistics \
    --namespace AWS/SES \
    --metric-name SendCount \
    --dimensions Name=ses:multi-region-endpoint-id,Value=abcdef12.g3h \
    --start-time 2024-10-01T00:00:00Z \ --end-time 2024-10-31T23:59:59Z \
    --period 86400 \
    --statistics Sum
```

abcdef12.g3h Remplacez-le par votre identifiant de point de terminaison actuel.

Bonnes pratiques et considérations

Le respect de ces meilleures pratiques et considérations permet de garantir une utilisation, une surveillance et une optimisation des coûts efficaces des points de terminaison mondiaux sur plusieurs sites afin Régions AWS d'améliorer la disponibilité et la fiabilité des capacités d'envoi d'e-mails.

- Synchronisez régulièrement les modifications apportées aux artefacts (par exemple, les ensembles de configuration, les identités vérifiées) entre les régions afin de préserver l'intégrité des envois.
- Surveillez les Cross-region indicateurs pour garantir une répartition équilibrée du trafic et identifier les problèmes potentiels.
- Sachez qu'il peut y avoir une augmentation fractionnée de la latence des API lorsque vous passez des appels vers des régions MREP-enabled éloignées.
- Pour garantir une répartition équilibrée du trafic, adoptez une architecture active-active qui reflète les régions de votre point de terminaison mondial. Vous pouvez également choisir deux régions à peu près également éloignées de votre application client.
- Configurez votre application cliente pour détecter rapidement les modifications de routage. Les points de terminaison mondiaux publient les pondérations de routage actuelles via le DNS. Définissez le TTL du cache DNS positif à environ 60 secondes et le TTL du cache DNS négatif à environ 10 secondes dans votre configuration d'exécution et de résolution. Sur la JVM, ils sont contrôlés par les propriétés de `networkaddress.cache.negative.ttl` sécurité `networkaddress.cache.ttl` et.
- Définissez les limites de durée de vie des connexions HTTP dans votre client. Long-lived les connexions keep-alive continuent d'atteindre l'adresse IP initialement résolue même après les actualisations du DNS. Définissez un [TTL de connexion](#) court d'environ 60 secondes sur votre client HTTP afin que les connexions groupées soient régulièrement remplacées. La plupart des AWS SDK exposent ce paramètre.
- Les points de terminaison globaux ne prennent pas en charge l'accès aux points de terminaison SMTP ou VPC.
- Tenez compte des éventuels frais de sortie si vous acheminez le trafic via une passerelle NAT.

Tarification

Bien que les détails exacts des prix soient sujets à modification, les terminaux internationaux devraient proposer un tarif plus élevé par rapport à l'envoi d'un volume de courrier dans une seule

région. Malgré cette augmentation, le coût global devrait rester compétitif par rapport aux autres fournisseurs de services de courrier électronique.

Pour obtenir les informations tarifaires les plus récentes, consultez la [page de tarification d'Amazon SES](#).

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 de celles 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

Avantage	Adresses IP partagées	Adresses IP dédiées (standard)	Adresses IP dédiées (gérées)
Isolation de la réputation par type d'e-mail, destinataire ou d'autres facteurs	Non	Oui	Oui
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 des situations où vos habitudes d'envoi sont très irrégulières, l'utilisation d'adresses IP dédiées (gérées) est la meilleure option.

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.

Note

Pour plus d'informations sur les données SNDS (Smart Network Data Services) pour votre service dédié IPs (standard), consultez [Métriques SNDS pour les applications dédiées IPs](#).

Adresses IP dédiées (gérées) : après le préchauffage de votre nouvelle adresse IPs, 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.

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 d'entre eux ISPs ne surveillent la réputation d'une adresse IP donnée que s'ils reçoivent un volume important de courrier provenant 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](#).

Les adresses IP dédiées (gérées) sont disponibles moyennant des frais mensuels standard (quel que soit le montant IPs nécessaire) et 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, une solution dédiée IPs (gérée) surveille 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 votre courrier sur la IPs page dédiée 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. Alors que SES gère le dimensionnement automatique de votre pool d'adresses IP, vous pouvez consulter toutes les adresses IP dédiées actuellement attribuées à votre compte via la console ou l'API SES. Le nombre de personnes IPs dans votre pool continuera d'augmenter ou de diminuer de manière dynamique en fonction de votre demande d'envoi.

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 “Adresses IP dédiées \(gérées\)”](#). En plus de vous permettre de contrôler totalement votre réputation d'expéditeur à l'aide d'adresses IP dédiées, les adresses IP dédiées IPs (standard) vous permettent de gérer entièrement vos adresses dédiées IPs, notamment de les réchauffer, de les étendre et de gérer le pool d'adresses IP.

Dédiée IPs (standard) et dédiée IPs (gérée) font toutes deux référence aux adresses IP dédiées que vous louez dans SES moyennant des [frais supplémentaires](#), mais elles diffèrent quant à la manière dont elles sont mises en œuvre et gérées. 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 le service dédié IPs (standard) dans SES.

Rubriques

- [Demande et abandon d'adresses IP dédiées \(standard\)](#)
- [Préparation des adresses IP dédiées \(standard\)](#)
- [Création de pools d'adresses IP dédiés standard pour les serveurs dédiés IPs \(standard\)](#)

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 renoncez à un service dédié IPs \(standard\) par le biais du AWS Support Centre](#). 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 lors de l'utilisation de la IPs solution dédiée (standard).

Pour plus d'informations sur les coûts associés au service dédié IPs (standard), consultez la section [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 disponibles dans chacune d'elles Région AWS, consultez la section [Infrastructure AWS mondiale](#).

Demande ou renonciation à un service dédié IPs (standard)

Vous pouvez demander autant de demandes dédiées IPs (standard) que vous le souhaitez en créant un dossier d'augmentation du quota de service dans le AWS Support Center.

Pour demander ou renoncer à un service dédié IPs (standard)

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 Dedicated IPs.
3. Effectuez l'une des actions suivantes :
 - a. Si vous n'avez pas encore de service dédié IPs dans votre compte :
 - La page IPs d'accueil dédiée s'affiche. Dans le panneau de présentation dédié IPs (standard), choisissez Request dedicated IPs.
 - b. Si vous avez déjà IPs un compte dédié :
 - i. Sélectionnez l'onglet Pools IP standard sur la IPs page dédiée.
 - ii. Dans le panneau de présentation standard, choisissez Request or relinquish Standard dedicated. IPs
4. Le Hello ! Nous sommes là lorsque la page d'aide s'ouvre dans la console de AWS support. Les valeurs suivantes seront présélectionnées pour tous les champs de cette page :
 - Choisissez le problème correspondant à votre cas — Compte et facturation
 - Service — Quotas de service
 - Catégorie — Amazon SES
 - Gravité — Question générale

Après avoir vérifié ces valeurs, choisissez Étape suivante : Informations supplémentaires.

5. Sous Informations supplémentaires, effectuez les sélections suivantes :
 - Pour Région, sélectionnez Région AWS celle à laquelle s'applique votre demande.
 - Pour le titre du quota, sélectionnez l'adresse IP dédiée souhaitée.

- Dans **Value**, sélectionnez le nombre de véhicules dédiés IPs que vous demandez ou que vous abandonnez dans la région sélectionnée.
- Si vous souhaitez demander ou renoncer à une limite dédiée IPs (standard) dans une autre Région AWS, choisissez **Ajouter une autre limite** et remplissez les champs en conséquence. Répétez l'opération pour chaque élément supplémentaire Région AWS.
- Dans **Description**, indiquez clairement ce que vous avez et ce que vous voulez faire dans chaque région spécifiée, comme dans les exemples suivants :

Demande — « J'en ai deux DIPs dans la région de Milan, mais j'aimerais en ajouter une de plus pour un total de trois »

Renoncez — « J'en ai deux DIPs dans la région de l'Ohio, mais je souhaite supprimer l'un d'entre eux. Veuillez supprimer le DIP dont l'adresse est 23.251.228.95 ».

 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.

- Choisissez **Next step: Solve now or contact us** (Étape suivante : résolvez maintenant ou contactez-nous).
- Sur la page **Résoudre maintenant** ou **Contactez-nous**, sélectionnez la langue de contact de votre choix, puis choisissez **Soumettre**.

Une fois le formulaire envoyé, nous évaluons votre demande. Si nous accédons à votre demande, nous répondrons à votre demande dans le Centre de Support pour confirmer que les adresses IP dédiées ont été ajoutées ou supprimées de votre compte conformément à votre demande.

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](#).

Préchauffage automatique pour une utilisation dédiée IPs (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 réchauffe automatiquement votre adresse dédiée IPs en augmentant progressivement le nombre d'e-mails que vous envoyez via votre adresse dédiée sur la IPs base d'un plan de préchauffage prédéfini. Cette augmentation progressive vous aide à vous IPs forger une réputation positive auprès des fournisseurs de services Internet (ISPs).

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 une adresse dédiée IPs (standard) pour la première fois, SES répartit vos e-mails envoyés entre vos adresses IP dédiées et un ensemble d'adresses partagées avec d'autres clients de 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 les e-mails que vous envoyez entre votre adresse dédiée existante IPs (qui est déjà réchauffée) et votre nouvelle adresse dédiée IPs (qui n'est pas réchauffée). 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.

Désactiver le processus de préchauffage automatique sur un appareil dédié IPs (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 préchauffage automatique, tous les objets dédiés loués ultérieurement IPs seront ajoutés à votre compte avec le statut de préchauffage terminé, ce qui les rendra utilisables sans avoir été réchauffés. Cela signifie que vous êtes responsable de vous assurer qu'ils IPs sont correctement réchauffés avant de les utiliser pour des envois réguliers. Tout IPs ce qui était en cours de préchauffage au moment où vous avez désactivé la fonction de préchauffage automatique ne sera pas affecté.

 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 préchauffage automatique pour tous les appareils dédiés IPs (standard) 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 Dedicated IPs.
3. Sélectionnez l'onglet Pools IP standard sur la IPs page dédiée.
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.

Réchauffement manuel dédié IPs (standard)

Vous pouvez augmenter ou diminuer manuellement votre volume d'envoi actuel dédié IPs (standard) en modifiant son pourcentage de préchauffage, en mettant fin à son processus de préchauffage prématurément, en réglant son volume d'envoi actuel sur 0 % et en relançant le processus de préchauffage.

Pour réchauffer manuellement un appareil dédié IPs (standard)

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 Dedicated IPs.
3. Sélectionnez l'onglet Pools IP standard sur la IPs page dédiée.
4. Dans le IPs panneau dédié All Standard, sélectionnez une adresse IP, choisissez Modifier le préchauffage, puis 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. Pourcentage de réinitialisation : lisez le pourcentage de réinitialisation de l'échauffement ? dialogue pour confirmer que vous réglez le volume d'envoi actuel de l'adresse IP à 1 % et que vous devrez soit redémarrer le processus de préchauffage automatique, soit régler le pourcentage de préchauffage manuellement, puis choisir Réinitialiser.

La colonne Warm-up status (Statut de préparation) indique In progress et la colonne Warm-up percentage (Pourcentage de préparation) affiche 1%.

Création de pools d'adresses IP dédiés standard pour les serveurs dédiés IPs (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 des applications dédiées IPs (standard) dans un pool 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 pool d'adresses IP dédié IPs (standard) 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 volet de navigation de gauche, choisissez Dedicated IPs.

 Note

Si vous n'avez actuellement aucun service dédié IPs (standard) IPs sur votre compte, la page d'accueil dédiée s'affiche pour vous permettre d'acheter du logiciel dédié IPs (standard). Pour de plus amples informations, veuillez consulter [the section called "Demande ou renonciation à un service dédié IPs \(standard\)"](#).

3. Sélectionnez l'onglet Pools IP standard sur la IPs page dédiée.
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 la fonction dédiée IPs (gérée) dans votre compte, il vous suffit de créer un pool d'adresses IP géré et SES s'occupe du reste. SES déterminera le nombre de personnes dédiées dont IPs vous avez besoin en fonction de vos habitudes d'envoi, les créera pour vous, puis gèrera leur mise à l'échelle en fonction de vos besoins d'envoi.

Une fois activé, vous pouvez utiliser le service dédié IPs (géré) dans l'envoi de vos e-mails en associant le pool d'adresses IP géré à un [ensemble de configuration](#), puis en spécifiant ce jeu de configuration 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 du service dédié IPs (géré)

Les adresses IP dédiées que vous créez avec des tâches de gestion dédiées IPs (gérées) automatisent les tâches de gestion afin de garantir que vos adresses IP dédiées sont utilisées de manière optimale pour la manière dont vous envoyez des e-mails :

- **Intégration simplifiée** — Pour commencer à utiliser le service dédié IPs (géré), vous devez créer un pool d'adresses IP géré directement depuis 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.
- **Échauffement intelligent** : commencez à envoyer des e-mails à des destinataires dédiés IPs (gérés) en ISPs 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 dédiée IPs (gérée) fournit des informations sur votre réputation à un taux

quotidien effectif, avec ISPs les meilleures CloudWatch statistiques Amazon et des 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 avez envoyé tout votre trafic vers Gmail, les adresses IP sont considérées comme réchauffées uniquement pour Gmail et froides pour les autres ISPs. 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 le IPs protocole dédié (géré) réchauffe 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 votre nouveau client dédié IPs pendant qu'il est en cours de préchauffage, SES répartira automatiquement une partie de vos envois dans le pool d'adresses IP partagées de SES afin de protéger la réputation de votre nouveau client dédié IPs.
 - Même une fois que votre nouveau site dédié IPs est complètement réchauffé, il n'est pas garanti que tous vos envois y passeront 100 % du temps. Par exemple, si votre taux d'envoi augmente soudainement et que IPs Dedicated (géré) détermine qu'il doit allouer une adresse IP dédiée supplémentaire, il 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 d'adresses IP partagées de SES, voir [the 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 IPs (standard). Lors de l'intégration avec des

adresses IP dédiées IPs (gérées) directement depuis la console, la CLI ou l'API SES, des adresses IP dédiées vous sont automatiquement attribuées et des frais vous sont facturés en fonction du volume de messages que vous envoyez. Lorsque vous supprimez un pool d'adresses IP créé par dedicated IPs (géré) ou que vous désactivez le pool dédié IPs (géré), les adresses IP qui vous ont été attribuées sont automatiquement annulées et les frais cessent immédiatement.

- Obtenir votre première adresse IP dédiée — La fonctionnalité dédiée IPs (gérée) attribuera automatiquement votre première adresse IP dédiée une fois que votre volume d'envoi atteindra des centaines de courriels 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 garantir que votre e-mail sera livré via votre adresse IP dédiée, celle-ci doit avoir une bonne réputation auprès du fournisseur de services Internet destinataire. ISPs n'accepteront qu'un petit volume d'e-mails provenant d'une adresse 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 l'attribution d'une adresse IP dédiée IPs (gérée), elle lance le processus de [préchauffage intelligent](#).

Grâce aux fonctionnalités [Warmup per ISP](#) et [Adaptive Warmup](#) dédiées IPs (gérées), la continuité des activités est maintenue tout au long du cycle de préchauffage en garantissant la livraison de votre courrier électronique. 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 maintenir la réputation IP, une adresse IP dédiée IPs (gérée) peut supprimer votre adresse IP dédiée et votre envoi sera acheminé 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. Vérifiez si le mode dédié IPs (géré) convient à la façon dont vous envoyez des e-mails en consultant le tableau de comparaison dans [Adresses IP dédiées](#).

Comprendre la responsabilité partagée entre vous et SES lors de l'utilisation de solutions dédiées IPs (gérées)

Bien que les adresses IP dédiées (gérées) offrent de nombreuses fonctionnalités automatisées pour la gestion, le dimensionnement et le préchauffage des adresses IP dédiées, l'étendue de cette automatisation et les responsabilités des SES doivent être comprises. Il serait faux de supposer que « géré » signifie que SES gère complètement tous les aspects liés à la réputation de propriété intellectuelle et aux problèmes de cotation. Pour clarifier ces idées fausses, nous devons souligner que même si le service automatise les aspects techniques tels que la mise à l'échelle et le préchauffage, vous restez responsable du maintien de votre réputation d'expéditeur et de la gestion des problèmes liés à la réputation, tels que l'inscription sur une liste de blocage de réputation (RBL).

Ce qui suit FAQs clarifie le modèle de responsabilité partagée entre vous et SES et dissipe les idées fausses courantes concernant la portée du service. Ces FAQ soulignent que même si l'aspect « géré » fait référence à la gestion de l'infrastructure technique, vous devez toujours surveiller et préserver activement votre réputation d'expéditeur, maintenir des taux de rebond bas et traiter vous-même la plupart des demandes de radiation RBL :

- [the section called “DIPS géré FAQs”](#)

Création d'un pool d'adresses IP géré pour activer le service dédié IPs (géré)

Pour activer le service dédié IPs (géré), vous devez d'abord créer un pool d'adresses IP géré. Une fois que vous avez créé un pool géré, la fonctionnalité détermine le nombre de personnes dédiées dont IPs vous avez besoin en fonction de vos habitudes d'envoi et les adapte dynamiquement 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 volet de navigation de gauche, choisissez Dedicated IPs.
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. Si vous n'avez pas encore de service dédié IPs dans votre compte :
 - La page IPs d'accueil dédiée s'affiche. Dans le panneau de présentation dédié IPs (géré), choisissez Activer le service dédié IPs.

La page Create IP Pool (Créer un groupe d'adresses IP) s'ouvre.
 - b. Si vous avez déjà IPs un compte dédié :
 - i. Sélectionnez l'onglet Pools d'adresses IP gérés sur la IPs page dédiée.
 - 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 le service dédié IPs (géré), 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 Pools IP standard sur la IPs page dédiée.
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. Tous vos fichiers dédiés actuels IPs (standard) seront déplacés vers le pool géré.
 2. Si vous louez actuellement un trop grand nombre de produits dédiés IPs (standard) par rapport à votre volume d'envoi, le service dédié IPs (géré) supprimera le redondant IPs.
 3. Si l'une de vos applications dédiées IPs (standard) figure sur une liste d'autorisation pour d'autres applications, vous ne devez pas les transférer vers le pool géré car elles seront supprimées si elles deviennent redondantes. Reportez-vous au point 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 de plus amples informations, veuillez consulter [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 volet de navigation de gauche, choisissez Dedicated IPs.
3. Sélectionnez l'onglet Pools d'adresses IP gérés sur la IPs page dédiée.
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 :

- État d'envoi — Indique si le volume et la fréquence de vos envois sont suffisants pour utiliser IPs Dedicated en affichant l'un des deux statuts suivants :
 - Volume insuffisant – Votre volume d'envois est trop faible.
 - Envoi via Dedicated IPs — Un ou plusieurs IPs outils dédiés sont utilisés dans votre pool géré.
- Volume d'envoi d'adresses IP dédiées gérées : volume d'e-mails envoyés via IPs Dedicated dans votre pool géré au cours des 7 derniers jours.
- Pourcentage d'envoi d'adresses IP dédiées gérées : pourcentage d'e-mails envoyés via IPs Dedicated dans votre pool géré au cours des 7 derniers jours.

b. Graphiques :

- Volume envoyé : volume d'e-mails envoyés au cours des 7 derniers jours par le biais d'une solution dédiée IPs gérée par rapport à un envoi partagé IPs.

- Pourcentage du volume envoyé : pourcentage d'e-mails envoyés au cours des 7 derniers jours par le biais d'une gestion dédiée IPs par rapport à un e-mail partagé IPs.
 - Capacité du fournisseur de services Internet : affiche la quantité d'e-mails envoyés via un service dédié IPs de votre pool géré par rapport aux 10 e-mails les plus utilisés ISPs et leur capacité disponible lors de votre 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 :

- Envoyer : volume d'e-mails envoyés à la fois par le biais de sites gérés, dédiés IPs et partagés IPs.
- ApproximateDedicatedSendingPercentage— Indique le pourcentage approximatif du trafic qui a été 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 pool d'adresses IP géré et désactivation du pool dédié IPs (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 disposez que d'un seul pool d'adresses IP géré et que vous le supprimez, ou si vous supprimez le dernier pool d'adresses IP géré restant, vous désactiverez la fonctionnalité dédiée IPs (gérée) et les frais cesseront immédiatement.

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 volet de navigation de gauche, choisissez Dedicated IPs.
3. Sélectionnez l'onglet Pools d'adresses IP gérés sur la IPs page dédiée.
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 pool géré ou si vous supprimez votre dernier pool géré, la fenêtre contextuelle vous rappellera qu'en supprimant le pool géré restant, vous désactiverez la fonctionnalité dédiée IPs (gérée) et ne serez plus facturée pour celle-ci. 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

Le BYOIP n'est disponible que pour les adresses IP dédiées que vous configurez manuellement ; il ne peut pas être utilisé avec Dedicated (géré). IPs

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.

Exigences

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 une autre plage Service AWS pour le BYOIP, telle 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 sous une autre forme Région AWS ou en créer une nouvelle 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 d'adresses IP avec Amazon SES, envoyez les informations suivantes à ses-byoip-request@amazon.com :

- L'identifiant AWS de votre compte.
- Celui dans Région AWS lequel vous souhaitez utiliser la plage d'adresses IP, par exemple 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 garantir 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 de courrier électronique réussie. Virtual Deliverability Manager est une fonctionnalité d'Amazon SES qui vous aide à améliorer la délivrabilité des e-mails en fournissant des informations sur vos données d'envoi et de livraison, et en fournissant des conseils sur la manière de résoudre les problèmes qui ont une incidence négative sur le taux de réussite de vos livraisons et votre réputation.

Virtual Deliverability Manager propose deux ensembles complémentaires de fonctionnalités de délivrabilité :

Délivrabilité du SES

La délivrabilité de SES fournit des informations et des recommandations pour les e-mails envoyés via Amazon SES, ce qui vous aide à surveiller les taux de livraison, à suivre l'engagement, à identifier les problèmes de réputation et à résoudre les problèmes de configuration qui affectent le placement des boîtes de réception. Il comprend un tableau de bord permettant de consulter les données de délivrabilité au niveau du compte, du fournisseur de services Internet, de l'identité d'envoi et des paramètres de configuration, ainsi qu'un conseiller qui identifie les problèmes d'infrastructure et recommande des solutions. Consultez [the section called “Délivrabilité du SES”](#).

Délivrabilité globale

La délivrabilité mondiale étend votre visibilité au-delà d'Amazon SES grâce à des analyses basées sur un échantillon représentatif de vos envois, auprès de tous les fournisseurs via lesquels vos domaines envoient, et pas seulement Amazon SES. Il inclut l'analyse des campagnes, les taux de placement des boîtes de réception, les tests de placement des boîtes de réception et le suivi des listes de blocage. Consultez [the section called “Délivrabilité globale”](#).

Rubriques

- [Délivrabilité du SES](#)
- [Délivrabilité globale](#)

Délivrabilité du SES

La délivrabilité de SES fournit des informations et des recommandations pour les e-mails envoyés via Amazon SES, ce qui vous aide à surveiller les taux de livraison, à suivre l'engagement, à identifier les problèmes de réputation et à résoudre les problèmes de configuration qui affectent le placement des boîtes de réception.

La délivrabilité de SES est activée au niveau du compte lorsque vous activez Virtual Deliverability Manager via l'assistant d'intégration de la console Amazon SES.

Fonctionnalités principales

La délivrabilité de SES inclut les fonctionnalités suivantes :

- **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. Cela vous permet d'identifier rapidement les domaines et les tendances problématiques, et de détecter les problèmes éventuels avant qu'ils ne se transforment en problèmes de délivrabilité plus importants, tels que des reports ou des blocages. Consultez [the section called “Tableau de bord”](#).
- **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 recommande des solutions pour résoudre des problèmes spécifiques liés à l'infrastructure de votre domaine d'envoi, de votre espace IP et de vos enregistrements d'authentification. Consultez [the section called “Conseiller”](#).

Prise en main

Pour commencer à utiliser la délivrabilité de SES, activez Virtual Deliverability Manager depuis l'assistant d'intégration de la console Amazon SES. Consultez [the section called “Prise en main”](#).

Rubriques

- [Démarrer avec Virtual Deliverability Manager](#)
- [Tableau de bord Virtual Deliverability Manager](#)
- [Conseiller Virtual Deliverability Manager](#)
- [Paramètres de Virtual Deliverability Manager](#)

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.

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 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 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.

Vous pouvez également activer la délivrabilité globale depuis la page des paramètres de Virtual Deliverability Manager pour étendre votre visibilité grâce à des analyses sur tous les fournisseurs. Consultez [the section called “Prise en main”](#).

Commencer à utiliser Virtual Deliverability Manager à l'aide du AWS CLI

Les exemples suivants décrivent comment démarrer avec Virtual Deliverability Manager à l'aide de l'AWS CLI.

Pour commencer à utiliser Virtual Deliverability Manager à l'aide du 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 à partir du AWS CLI, comme indiqué 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 ensemble de configurations utilisera le suivi des engagements et la diffusion partagée optimisée en remplaçant la façon dont ils ont été définis dans Virtual Deliverability Manager, consultez l' AWS CLI exemple dans [the section called "Settings"](#)

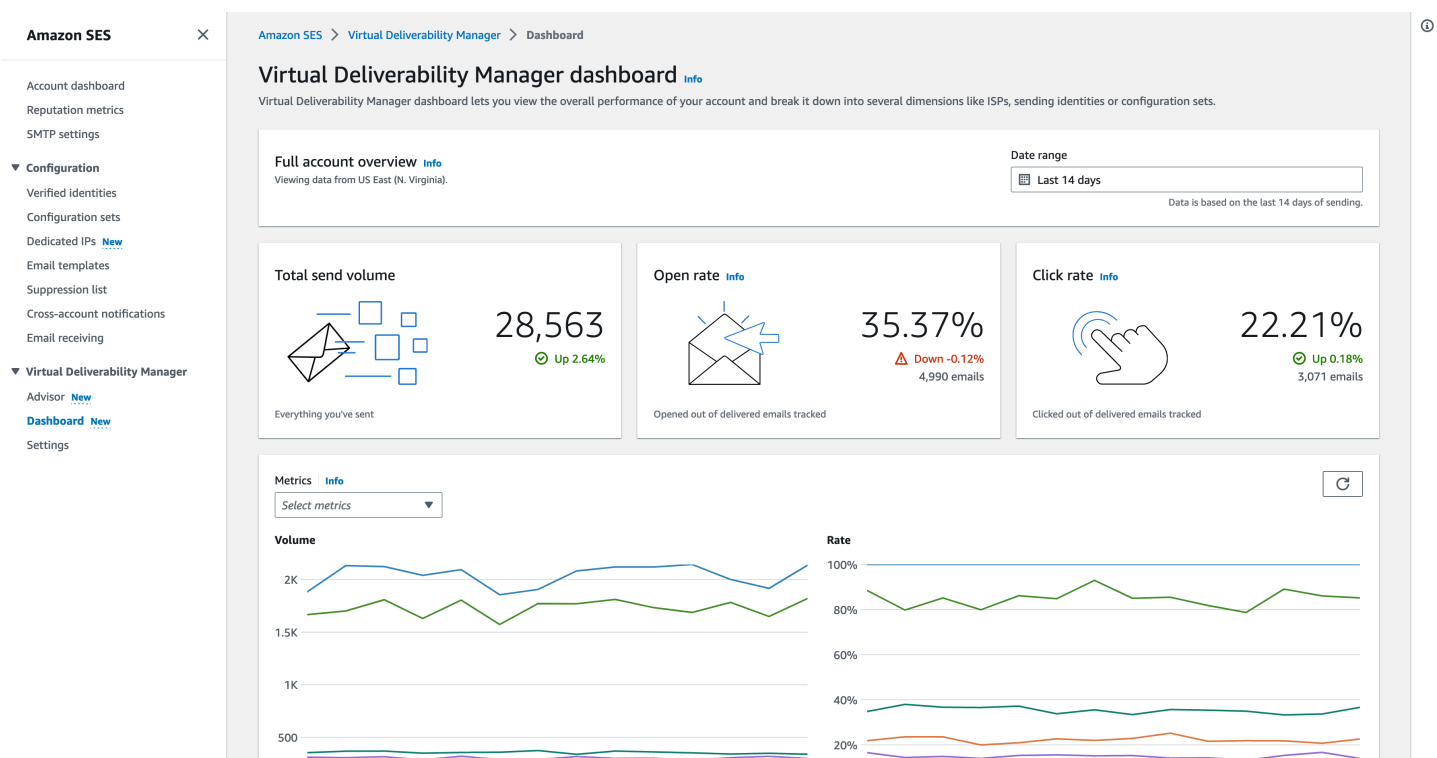
Tableau de bord Virtual Deliverability Manager

Le tableau de bord offre des vues de haut niveau du programme de délivrabilité de votre compte, telles que des fiches faciles à lire et des graphiques chronologiques qui montrent la délivrabilité et la réputation, ainsi que les taux de livraison open/click et les statistiques. bounce/complaint Le tableau de bord offre également une vue plus détaillée, qui vous permet d'accéder à des données de tableau

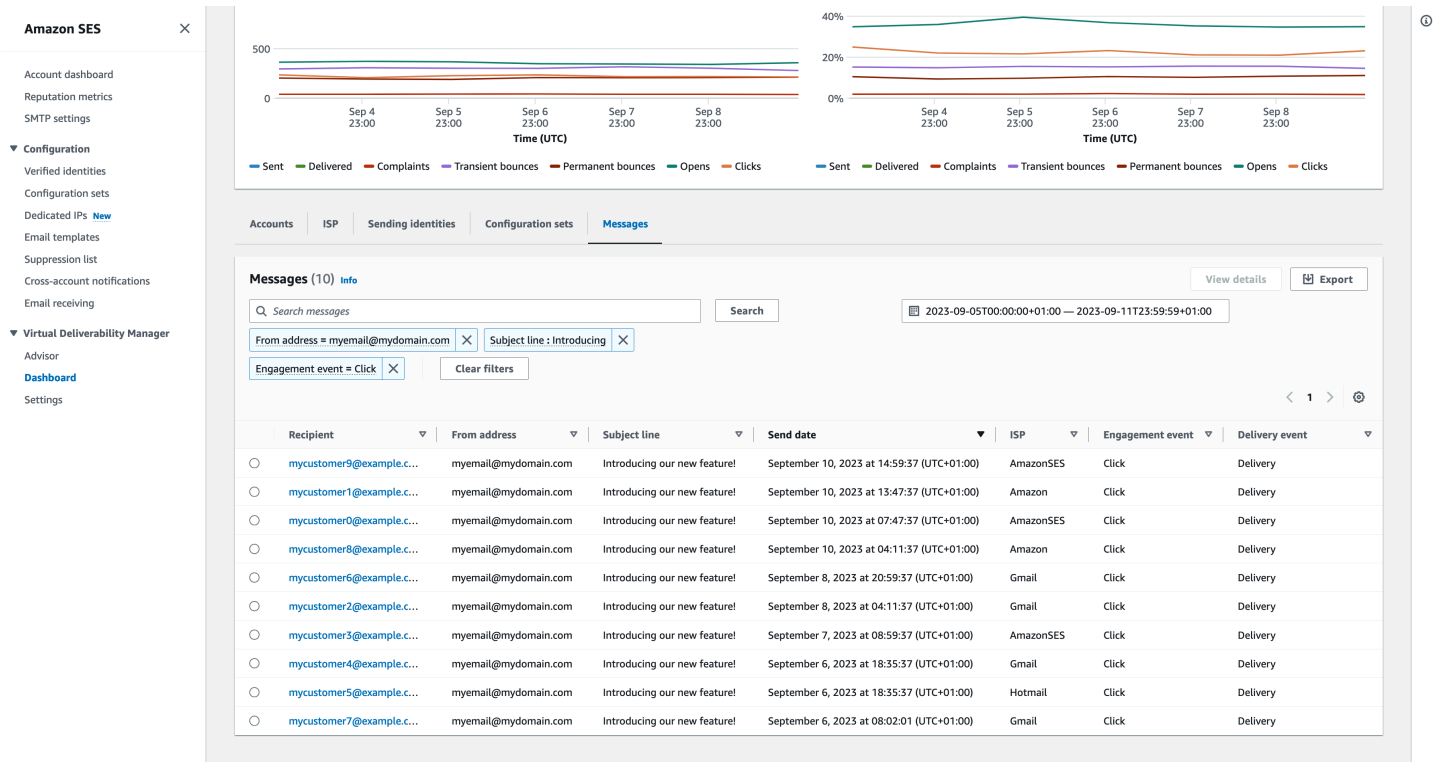
plus détaillées en cas de problème lié à un FAI, à une identité d'envoi ou à un jeu de configurations associé à une campagne par e-mail.

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.

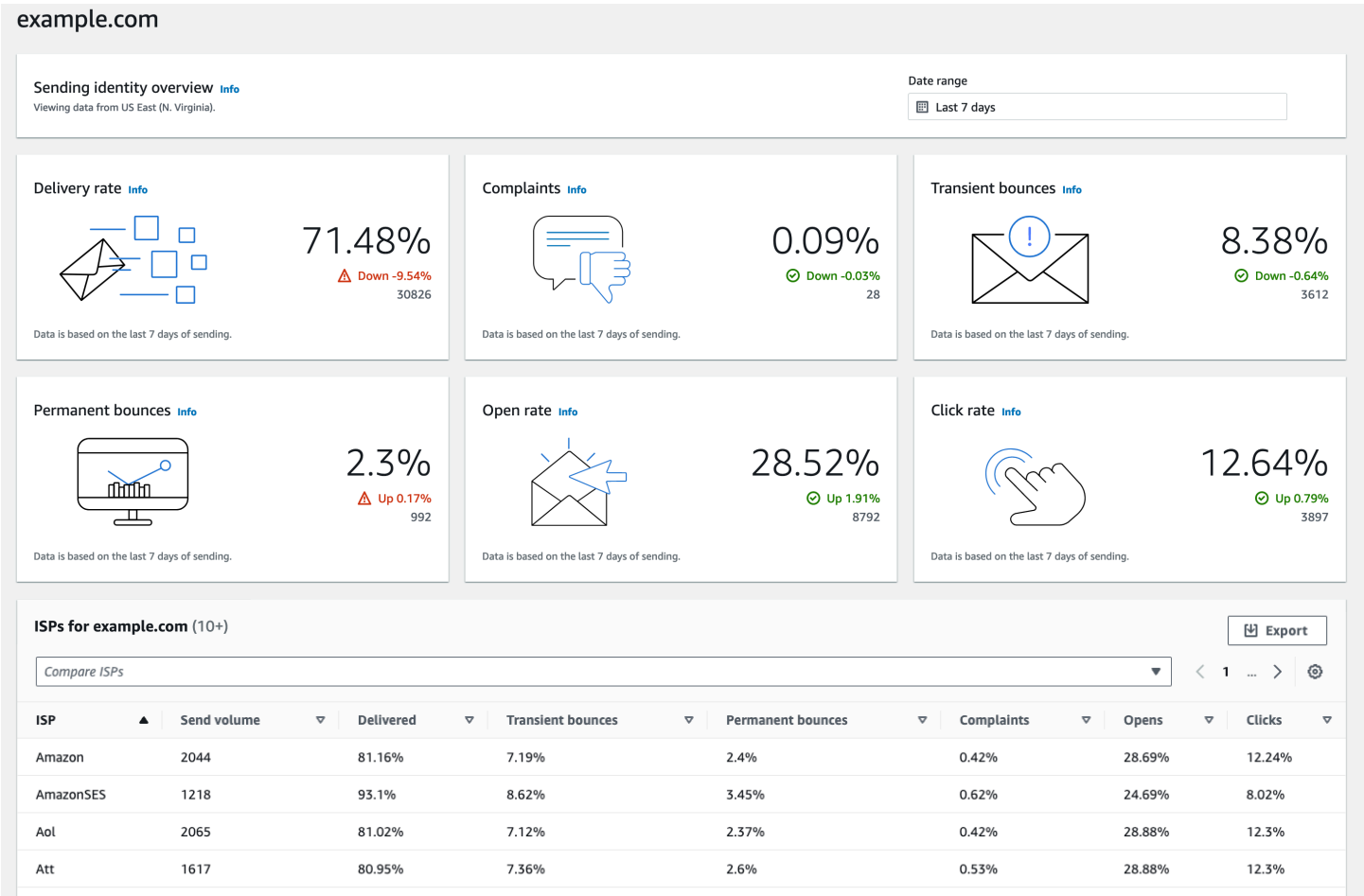


La table Messages sélectionnée dans le tableau de bord Gestionnaire virtuel de diffusion présentant les messages envoyés correspondant à la plage de dates et aux critères de filtrage.



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.

Drill-down données affichées dans le tableau de bord de Virtual Deliverability Manager pour l'identité d'envoi sélectionnée, example.com : les cartes affichent les indicateurs 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.



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 de plus amples informations, veuillez consulter [the section called “Prise en main”](#).
- Les statistiques du tableau de bord sont affichées en temps quasi réel.
- Les messages du tableau de bord s'affichent quelques minutes après leur envoi.

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 aux données métriques de votre Virtual Deliverability Manager à l'aide du 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 & d'engagement de livraison 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.

Gérez vos tâches d'exportation à l'aide du 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-deb5bbf2bfbf-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 activés 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				✓

Rate % (% du taux)	Comment le calculer	Avec le suivi des engagements activés 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
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 : Apple a mis en œuvre sa fonctionnalité de protection de la confidentialité des e-mails (MPP) sur les appareils Apple à partir d'iOS15, les numéros d'engagement ont augmenté à mesure que les déclencheurs MPP s'ouvrent lorsque l'application Apple Mail est lancée, pas nécessairement lorsqu'un destinataire ouvre un message et clique sur un message. and/or 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 et l'utilisation du Web, ainsi que l'app/portal utilisation de données proxy provenant d'appareils autres qu'Apple pour créer un indicateur agrégé. 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 inexistantes 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.

Amazon SES > Virtual Deliverability Manager > Advisor

Virtual Deliverability Manager advisor [Info](#)

Virtual Deliverability Manager advisor lets you optimize your email deliverability and engagement by identifying key performance issues and how to resolve them accordingly.

[Open recommendations](#) | Resolved recommendations

Open recommendations (10+) [Info](#)

Q Search recommendations

Impact	Identity name	Age	Recommendation/Description	Last checked	Resolve issue
High	example1.com	2 days	DKIM verification is not enabled.	10 minutes ago	Setting up DKIM records
High	example2.com	2 days	DKIM verification has failed.	10 minutes ago	Setting up DKIM records
High	example3.com	2 days	DKIM signing key length is below 2048 bits.	10 minutes ago	Setting up DKIM records
High	example9.com	4 days	SPF record was not found.	36 minutes ago	Setting up SPF records
High	example10.com	4 days	SPF record for Amazon SES was not found.	36 minutes ago	Setting up SPF records
Low	example4.com	2 days	DMARC configuration was not found.	10 minutes ago	Setting up DMARC records
Low	example5.com	2 days	DMARC configuration could not be parsed.	10 minutes ago	Setting up DMARC records
Low	example6.com	2 days	DKIM record was not found.	10 minutes ago	Setting up DMARC records
Low	example7.com	4 days	BIMI record not found or configured without default selector.	36 minutes ago	Setting up BIMI
Low	example8.com	4 days	BIMI has malformed TXT record.	36 minutes ago	Setting up BIMI

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.

Si la délivrabilité globale est activée, le conseiller génère également des recommandations lorsque vos domaines ou adresses IP surveillés figurent sur une liste de blocage. Ces recommandations incluent le nom de la liste de blocage, le motif de l'inscription et les instructions de radiation. Pour de plus amples informations, veuillez consulter [the section called “Listes de blocage”](#).

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
Contrôle du taux de plaintes	<i>ISP_name</i> Le FAI a un taux de <i>high/med/low</i> plaintes.	Identity a dépassé le seuil de recommandations relatives aux plaintes pour ce fournisseur de services Internet.	Surveillance de la réputation d'expéditeur
Configuration DKIM	La vérification DKIM n'est pas activée.	Le DKIM n'est pas activé par identité.	Easy DKIM dans SES

Type de chèque	Message du conseiller	Pourquoi le conseiller vous alerte	EN SAVOIR PLUS
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
Configuration DKIM du DMARC	L'enregistrement DKIM n'est pas aligné.	Le domaine spécifié dans la signature DKIM ne correspond pas au domaine indiqué dans l'adresse d'origine.	Conformité au DMARC via DKIM

Type de chèque	Message du conseiller	Pourquoi le conseiller vous alerte	EN SAVOIR PLUS
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.	<code>include:a mazonses.com</code> est absent de l'enregistrement TXT SPF.	Configuration de votre domaine MAIL FROM personnalisé
Application du SPF configurée	Il manque le qualificatif SPF all.	<code>~all</code> est absent de l'enregistrement TXT SPF.	Configuration de votre domaine MAIL FROM personnalisé
Validation de l'application du SPF	Un problème de configuration SPF a été détecté.	Les tentatives de détection de l'enregistrement SPF MX requis dans les 72 heures ont échoué.	États de configuration 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 BIMl	BIMl a un enregistrement TXT mal formé.	L'enregistrement BIMl 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 BIMl

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 de plus amples informations, veuillez consulter [the section called "Prise en main"](#).

3. Open recommendations table (Tableau des recommandations ouvertes) s'affiche par défaut. Les recommandations sont classées par impact (High/Low), nom d'identité (domaine d'envoi), âge (de l'alerte) et Recommendation/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 Recommendation/Description colonne, cliquez sur le lien correspondant à cette ligne dans la colonne Résoudre le problème 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).

Accédez aux recommandations de votre Virtual Deliverability Manager à l'aide du 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

La page des paramètres de Virtual Deliverability Manager permet de contrôler à la fois la délivrabilité de SES et la délivrabilité globale. Vous pouvez consulter ou modifier les paramètres à tout moment à l'aide de la console Amazon SES ou du AWS CLI.

Paramètres de délivrabilité SES

Les paramètres de délivrabilité de SES contrôlent le suivi des engagements et optimisent la diffusion partagée au niveau du compte. Vous pouvez également définir des paramètres personnalisés au niveau du jeu de configuration pour remplacer les paramètres par défaut au niveau du compte.

Modification des paramètres de délivrabilité de SES à l'aide de la console Amazon SES

Pour modifier les paramètres de délivrabilité de SES 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 volet de navigation de gauche, choisissez Settings (Paramètres) sous Virtual Deliverability Manager.
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).

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 indiquant comment un ensemble de configurations utilise le suivi des engagements et la diffusion partagée optimisée en remplaçant la façon dont ils sont définis dans Virtual Deliverability Manager, faites référence aux [options de Virtual Deliverability Manager](#) lors de la création ou de la modification d'un ensemble de configuration.
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).
6. Pour réactiver Virtual Deliverability Manager, consultez [the section called "Prise en main"](#).

Modification des paramètres de délivrabilité de SES à l'aide du AWS CLI

Vous pouvez utiliser les [PutConfigurationSetVdmOptions](#) opérations [PutAccountVdmAttributes](#) et dans l'API Amazon SES v2 pour modifier vos paramètres de délivrabilité SES.

- 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 associés en établissant un lien à partir du type de [VdmAttributes](#) données dans la référence de l'API Amazon SES v2.

- Définissez des paramètres personnalisés indiquant comment un ensemble de configurations utilisera le suivi des engagements et la diffusion partagée optimisée en remplaçant la façon dont ils ont été définis 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.

Paramètres de délivrabilité globaux

Les paramètres de délivrabilité globaux contrôlent la surveillance des domaines, la surveillance IP et les tests de placement des boîtes de réception. La délivrabilité globale est activée par région depuis la page des paramètres de Virtual Deliverability Manager.

Pour gérer les paramètres de délivrabilité globaux 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 volet de navigation de gauche, choisissez Settings (Paramètres) sous Virtual Deliverability Manager.
3. Dans le panneau de délivrabilité globale, vous pouvez :
 - Activez ou désactivez la délivrabilité globale pour la région actuelle.
 - Choisissez Modifier les domaines pour sélectionner les domaines d'envoi vérifiés à surveiller.

Pour obtenir des instructions détaillées sur l'activation ou la désactivation de la délivrabilité globale, consultez [the section called “Prise en main”](#) Pour plus d'informations sur les fonctionnalités de délivrabilité globale, consultez [the section called “Délivrabilité globale”](#).

Délivrabilité globale

La délivrabilité mondiale étend votre visibilité au-delà d'Amazon SES. Il fournit des analyses basées sur un échantillon représentatif de vos envois, auprès de tous les fournisseurs via lesquels vos domaines envoient, et pas seulement Amazon SES.

Vous pouvez valider les campagnes avant leur expédition, suivre l'emplacement des boîtes de réception au niveau du fournisseur de services Internet et surveiller vos adresses IP et vos domaines par rapport aux principaux opérateurs de listes de blocage, le tout depuis la console Amazon SES.

La délivrabilité globale est activée par région. Quelle que soit la région, la surveillance des domaines permet de suivre les indicateurs par région, par compte et par fournisseur d'envoi. La surveillance IP

suit uniquement les adresses IP dédiées disponibles dans cette région. Les tests de placement dans la boîte de réception ne dépendent d'aucune région spécifique.

Fonctionnalités principales

La délivrabilité globale inclut les fonctionnalités suivantes :

- Analyse des campagnes : met en évidence les indicateurs de délivrabilité et d'engagement par campagne sur la base d'un échantillon représentatif d'e-mails envoyés depuis vos domaines surveillés, même lorsqu'ils sont envoyés par l'intermédiaire d'un fournisseur autre qu'Amazon SES. Consultez [the section called “Analyse de la campagne”](#).
- Taux de placement dans les boîtes de ISP-level réception : fournit les taux de placement des boîtes de réception pour vos domaines surveillés, mis à jour toutes les heures en fonction des analyses. Consultez [the section called “Taux de placement des boîtes de réception”](#).
- Tests de placement dans les boîtes de réception : envoie votre campagne aux comptes d'origine des principaux fournisseurs de boîtes aux lettres avant de l'envoyer à de vrais abonnés, afin que vous puissiez détecter à l'avance les problèmes de placement et d'authentification. Consultez [the section called “Tests de placement dans la boîte de réception”](#).
- Listes de blocage : surveille vos adresses IP dédiées et vos domaines d'envoi par rapport aux principaux opérateurs de listes de blocage du secteur grâce à des contrôles horaires et à des alertes proactives via Virtual Deliverability Manager Advisor lorsque quelque chose est répertorié (vous [pouvez les surveiller](#) via le logiciel). EventBridge Consultez [the section called “Listes de blocage”](#).

Tarification

La délivrabilité globale est vendue sous la forme d'un forfait d'abonnement unique comprenant des domaines surveillés, une surveillance IP dédiée et des tests de placement dans les boîtes de réception. Pour en savoir plus sur les tarifs, consultez la section [Tarification d'Amazon SES](#).

Prise en main

Pour commencer à utiliser la délivrabilité globale, activez-la depuis la page des paramètres de Virtual Deliverability Manager de la console Amazon SES. Consultez [the section called “Prise en main”](#).

Rubriques

- [Initiation à la délivrabilité mondiale](#)
- [Analyse de la campagne](#)

- [Taux de placement des boîtes de réception](#)
- [Tests de placement dans la boîte de réception](#)
- [Listes de blocage](#)

Initiation à la délivrabilité mondiale

Pour commencer à utiliser la délivrabilité globale, vous devez l'activer depuis la page des paramètres de Virtual Deliverability Manager de la console Amazon SES. Après l'activation, vous sélectionnez les domaines d'envoi vérifiés à surveiller.

Permettre la délivrabilité globale à l'aide de la console Amazon SES

Pour activer la délivrabilité globale 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 volet de navigation de gauche, choisissez Settings (Paramètres) sous Virtual Deliverability Manager.
3. Dans le panneau de délivrabilité globale, choisissez Activer la délivrabilité globale.
4. Dans la boîte de dialogue de confirmation, passez en revue les détails de l'abonnement et choisissez Activer la délivrabilité globale.

L'abonnement inclut des domaines surveillés, une surveillance IP dédiée et des tests de placement dans les boîtes de réception. Pour en savoir plus sur les tarifs, consultez la section [Tarification d'Amazon SES](#).

5. Après l'activation, choisissez Modifier les domaines pour sélectionner les domaines d'envoi vérifiés à surveiller.

Désactivation de la délivrabilité globale

Pour désactiver la délivrabilité globale 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 volet de navigation de gauche, choisissez Settings (Paramètres) sous Virtual Deliverability Manager.

3. Dans le panneau de délivrabilité globale, choisissez Désactiver la délivrabilité globale.
4. Dans la boîte de dialogue de confirmation, entrez *disable* dans le champ de confirmation, puis choisissez Désactiver la délivrabilité globale.

Important

La désactivation de la délivrabilité globale supprime l'accès aux analyses des campagnes, aux tests de placement dans les boîtes de réception et à la surveillance de la réputation.

Analyse de la campagne

L'analyse des campagnes met en évidence les indicateurs de délivrabilité et d'engagement par campagne sur la base d'un échantillon représentatif d'e-mails envoyés depuis vos domaines surveillés, auprès de tous les fournisseurs par lesquels vos domaines sont envoyés, et pas seulement Amazon SES. Utilisez l'analyse des campagnes pour identifier les campagnes les plus performantes et les points à améliorer.

Ce que fournit l'analyse des campagnes

Pour chaque campagne détectée, l'analyse des campagnes affiche les informations suivantes :

- **Objet** : objet de la campagne.
- **Adresse d'expéditeur** : adresse de l'expéditeur utilisée pour la campagne.
- **Date du dernier envoi** : date la plus récente à laquelle la campagne a été envoyée.
- **Messages envoyés** : nombre de messages envoyés dans le cadre de la campagne.
- **Taux de réception** : pourcentage de messages arrivés dans la boîte de réception.
- **Taux de spam** : pourcentage de messages envoyés comme spam.

Afficher les détails de la campagne

Lorsque vous sélectionnez une campagne dans la liste des campagnes, vous pouvez consulter des informations détaillées, notamment :

- **Détails de la campagne** : numéro de campagne, adresse du destinataire, adresse de l'expéditeur, messages envoyés, volume prévu, date de première consultation et date de dernière consultation.

- Mesures d'engagement : taux de boîte de réception, taux de spam, taux d'ouverture et taux de suppression pour la campagne.
- Répartition des fournisseurs de services Per-ISP Internet : statistiques indiquant le taux de boîte de réception, le taux de spam, le taux d'ouverture et le taux de suppression pour chaque principal fournisseur de messagerie (Gmail, Yahoo, Outlook, etc.).

Pour consulter les analyses des campagnes 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 volet de navigation de gauche, choisissez Campaign Analytics sous Délivrabilité globale dans la section Virtual Deliverability Manager.
3. Le tableau Campagnes affiche toutes les campagnes détectées pour vos domaines surveillés.
4. Choisissez le sujet d'une campagne pour consulter ses statistiques détaillées et la répartition des fournisseurs de services Internet.

Taux de placement des boîtes de réception

Les taux de placement dans les boîtes de ISP-level réception fournissent des données de placement dans les boîtes de réception pour les domaines surveillés. Ces données sont alimentées par des analyses et mises à jour toutes les heures. Ces statistiques sont basées sur un échantillon représentatif de données et ne reflètent pas le volume total d'e-mails envoyés.

Ce que les taux de placement dans les boîtes de réception

Pour chaque domaine surveillé, les taux de placement dans les boîtes de réception affichent les informations suivantes :

- ISP-level répartition : débit de boîte de réception, taux de spam, nombre de boîtes de réception et nombre de spams pour chaque principal fournisseur de boîtes aux lettres (Gmail, Outlook, Yahoo, etc.).
- Mesures agrégées : taux global de boîte de réception et taux de spam pour tous les fournisseurs de services Internet pour le domaine sélectionné.
- Données de tendance : graphique chronologique montrant les taux de placement des boîtes de réception par fournisseur de services Internet sur la plage de dates sélectionnée.

Afficher les taux de placement dans les boîtes de réception à l'aide de la console Amazon SES

Pour consulter les taux de placement dans les boîtes de réception 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 volet de navigation de gauche, choisissez Inbox placement rates sous Global Deliverability dans la section Virtual Deliverability Manager.
3. Sélectionnez un domaine surveillé dans le sélecteur de domaines.
4. (Facultatif) Réglez la plage de dates à l'aide du sélecteur de plage de dates. Vous pouvez sélectionner des plages relatives (7, 14, 30 ou 90 jours) ou spécifier une plage de dates absolue.
5. Consultez le tableau de répartition des fournisseurs de services Internet et le graphique des tendances pour identifier les fournisseurs de services Internet dont le placement des boîtes de réception est inférieur aux attentes.

Note

Les données de placement dans la boîte de réception sont fournies par des analyses et mises à jour toutes les heures. Ces statistiques sont basées sur un échantillon de données et ne reflètent pas le volume total d'e-mails envoyés.

Tests de placement dans la boîte de réception

Les tests de placement dans les boîtes de réception permettent à votre campagne de créer des comptes auprès des principaux fournisseurs de boîtes aux lettres avant de les envoyer à de vrais abonnés, afin que vous puissiez détecter les problèmes de placement et d'authentification avant qu'ils n'atteignent votre public. Les résultats sont généralement disponibles en 2 à 4 heures.

Ce que fournissent les tests de placement dans la boîte de

Chaque test terminé fournit les informations suivantes :

- Résultats globaux : pourcentage de boîtes de réception, pourcentage de spam et pourcentage de données manquantes pour tous les fournisseurs de services Internet testés.

- Répartition des fournisseurs de Per-ISP services Internet : boîte de réception, spam et pourcentages manquants pour Gmail, Outlook, Yahoo et d'autres grands fournisseurs.
- Détails du test : numéro du rapport, objet, adresse du formulaire, date de création et statut du test.

Votre abonnement mondial à la délivrabilité inclut des tests de placement dans votre boîte de réception tous les mois. Pour en savoir plus sur les prix, y compris les quantités incluses et les frais d'excédent, consultez la section [Tarification d'Amazon SES](#).

Création d'un test de placement dans la boîte de réception

Pour créer un test de placement dans la boîte de réception 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 volet de navigation de gauche, choisissez Inbox placement tests sous Livrabilité globale dans la section Virtual Deliverability Manager.
3. Choisissez Créer un test.
4. Sélectionnez l'identité à partir de laquelle envoyer. Vous pouvez choisir une adresse e-mail vérifiée ou spécifier une partie locale avec un domaine vérifié.
5. Entrez l'objet de l'e-mail de test.
6. Entrez le contenu de l'e-mail (HTML ou texte brut) que vous souhaitez tester.
7. Choisissez Créer un test.

Le test apparaît dans la liste des tests avec le statut En cours. Les résultats sont généralement disponibles en 2 à 4 heures.

Afficher les résultats des tests

Pour consulter les résultats des tests de placement dans la boîte de réception 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 volet de navigation de gauche, choisissez Inbox placement tests sous Livrabilité globale dans la section Virtual Deliverability Manager.
3. Choisissez le nom du test dans la liste des tests pour en afficher les détails.

4. Consultez la section Détails du test pour obtenir les résultats globaux et le tableau de répartition des fournisseurs de services Internet pour les données de placement par fournisseur.

Listes de blocage

La surveillance des listes de blocage surveille vos adresses IP dédiées et vos domaines d'envoi par rapport aux principaux opérateurs de listes de blocage du secteur, grâce à des contrôles horaires et à des alertes proactives via Virtual Deliverability Manager Advisor lorsque quelque chose est répertorié.

Opérateurs de listes de blocage surveillés

Global Deliverability surveille les opérateurs de listes de blocage suivants :

- Listes de blocage d'adresses IP — Surveille vos adresses IP dédiées par rapport aux principaux opérateurs de IP-based listes de blocage.
- Listes de blocage de domaines : surveille vos domaines d'envoi par rapport aux principaux opérateurs de listes de blocage basées sur des domaines.

Ce que fournit la surveillance des listes de blocage

La page des listes de blocage affiche les informations suivantes :

- Résumé — Le nombre de domaines et d'adresses IP surveillés, et le nombre d'entre eux figurant actuellement sur une liste de blocage.
- Domaines surveillés : tableau indiquant chaque domaine surveillé, son statut actuel (Listé ou Propre) et le nombre de listes de blocage sur lesquelles il apparaît.
- IP surveillées : tableau indiquant chaque adresse IP surveillée, son statut actuel et le nombre de listes de blocage sur lesquelles elle apparaît.
- Détails de l'inscription — Pour chaque entité répertoriée, le nom de la liste de blocage, la date d'inscription, le motif et la procédure de radiation, avec des liens directs vers le processus de suppression de l'opérateur de la liste de blocage.

Afficher le statut de la liste de blocage à l'aide de la console Amazon SES

Pour consulter l'état de la liste de blocage 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 volet de navigation de gauche, choisissez Blocklists sous Livrabilité globale dans la section Virtual Deliverability Manager.
3. Consultez la section Résumé pour obtenir un aperçu de l'état de votre surveillance.
4. Dans les tableaux Domaines surveillés ou IP surveillées, choisissez Afficher les détails de n'importe quelle entité pour afficher ses listes de blocage.
5. Pour les entités cotées, vérifiez le motif de l'inscription et suivez la procédure de radiation prévue pour demander leur retrait de la liste de blocage.

Note

Lorsqu'un domaine ou une adresse IP figure sur une liste de blocage, Virtual Deliverability Manager Advisor génère une recommandation contenant des conseils sur la manière de résoudre le problème. Pour plus d'informations, consultez [the section called “Conseiller”](#).

Validation des e-mails pour Amazon SES

La qualité des listes d'e-mails est un facteur essentiel pour maintenir des taux de livraison élevés et protéger la réputation de votre expéditeur. Les adresses e-mail non valides ou risquées peuvent entraîner des taux de rebond élevés, des plaintes pour spam, et les fournisseurs de boîtes aux lettres peuvent rejeter des e-mails, mettre des domaines d'envoi sur liste noire ou limiter les taux de livraison.

La validation des e-mails est une fonctionnalité d'Amazon SES qui vous permet de valider les adresses e-mail avant de les envoyer. Il vérifie les adresses e-mail pour détecter les erreurs de syntaxe, la validité du domaine et d'autres contrôles, et identifie les adresses risquées susceptibles de nuire à votre réputation d'expéditeur, vous aidant ainsi à maintenir des taux de délivrabilité élevés et à protéger votre réputation d'expéditeur.

Pourquoi la qualité et la validation des listes d'e-mails sont-elles importantes ?

Les fournisseurs de boîtes aux lettres surveillent les indicateurs clés tels que les taux de rebond, les taux de plaintes et les niveaux d'engagement pour évaluer la réputation de l'expéditeur. Lorsque ces indicateurs dépassent les seuils acceptables, les fournisseurs mettent en œuvre des mesures de protection telles que la limitation du débit, les reports temporaires ou les blocages permanents. Des taux de rebond élevés (généralement supérieurs à 5 à 10 %) sont le signe d'une mauvaise hygiène des listes et entraînent une atteinte immédiate à la réputation.

Les fournisseurs de boîtes aux lettres attendent des expéditeurs qu'ils maintiennent des listes d'e-mails propres et adoptent de bonnes pratiques d'envoi. Ils suivent les rebonds provenant d'adresses non valides, surveillent les pièges à spam et mesurent l'engagement des destinataires pour déterminer l'emplacement de la boîte de réception. La mauvaise qualité des listes se traduit par des impacts mesurables : réduction des taux de livraison, augmentation de la latence et possibilité d'une mise sur liste noire affectant toutes les futures campagnes provenant de votre domaine d'envoi ou de votre adresse IP.

Comment la validation des e-mails peut-elle améliorer la délivrabilité et la réputation ?

La validation des e-mails vous aide à améliorer à la fois votre délivrabilité et votre réputation grâce à une API qui vérifie les adresses e-mail à la demande, et à la validation automatique qui examine et filtre automatiquement les e-mails sortants en fonction des seuils de délivrabilité que vous avez définis.

- **Validation de l'API** : valide les adresses e-mail par le biais d'appels d'API, ce qui vous permet de valider les adresses au moment de la collecte, par exemple lors des formulaires d'inscription ou des processus d'abonnement, et pour le nettoyage périodique des listes de bases de données existantes. Cela permet d'empêcher les adresses non valides d'entrer dans votre base de données, de fournir des informations opportunes aux utilisateurs sur la validité des adresses et de maintenir régulièrement la qualité des listes d'e-mails.
- **Validation automatique** : examine automatiquement toutes les adresses e-mail sortantes et ne distribue les messages qu'aux destinataires qui atteignent le seuil de probabilité de livraison que vous avez sélectionné (élevé ou moyen). Cela protège la réputation de votre expéditeur en empêchant les envois vers des adresses non valides ou risquées sans intervention manuelle.

Rubriques

- [API de validation des e-mails](#)
- [Validation automatique](#)
- [Tableau de bord de validation des e-mails](#)

API de validation des e-mails

La validation des API vous permet de valider des adresses e-mail individuelles par le biais d'appels d'API, en fournissant des informations immédiates sur la validité des adresses, la délivrabilité et les facteurs de risque. Cette fonctionnalité est conçue pour valider les adresses au moment de la collecte, par exemple lors de l'enregistrement des utilisateurs, des formulaires d'abonnement ou dans tout autre scénario nécessitant des résultats de validation rapides.

La validation de l'API effectue plusieurs vérifications sur chaque adresse e-mail, notamment la validation de la syntaxe, la vérification du domaine, la vérification de l'existence des boîtes aux lettres, etc. Les résultats de validation incluent des verdicts de confiance (ÉLEVÉ, MOYEN ou FAIBLE) pour la validité globale et les évaluations individuelles.

Contrôles de validation effectués

La validation de l'API effectue les évaluations suivantes sur chaque adresse e-mail :

- **Validation de la syntaxe** (IsValidSyntax) — Vérifie que l'adresse e-mail respecte les normes RFC appropriées et contient des caractères valides au format correct.
- **Enregistrements DNS** (IsValidDnsRecords) : vérifie que le domaine existe, qu'il possède des enregistrements DNS valides et qu'il est configuré pour recevoir des e-mails.

- Existence d'une boîte aux lettres (MailboxExists« ») — Vérifie que la boîte aux lettres existe et qu'elle peut recevoir des messages sans envoyer d'e-mail.
- Adresse de rôle (« IsRoleAddress ») — Identifie les adresses basées sur les rôles (telles que admin@, support@ ou info@) susceptibles de présenter des taux d'engagement inférieurs.
- Domaine jetable (« IsDisposable ») — Vérifie les adresses e-mail jetables ou temporaires susceptibles d'avoir un impact négatif sur la réputation de votre expéditeur.
- Modèles de chaînes aléatoires (« IsRandomInput ») — Vérifie les modèles générés de manière aléatoire.

Utilisation de la validation d'API avec la console Amazon SES

La procédure suivante explique comment valider une adresse e-mail à l'aide de la console Amazon SES.

Pour valider une adresse e-mail 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 volet de navigation de gauche, choisissez Validation des adresses e-mail sous Validation des e-mails.
3. Dans la section Valider l'adresse e-mail, entrez l'adresse e-mail que vous souhaitez valider dans le champ Adresse e-mail.
4. Choisissez Valider.

Les résultats de validation apparaissent dans le panneau des résultats de validation, avec les informations suivantes :

- IsValid— Validité globale avec un verdict de confiance (ÉLEVÉ, MOYEN ou FAIBLE).
- Évaluations — Résultats d'évaluation individuels assortis de verdicts fiables concernant la syntaxe, les enregistrements DNS, l'existence de boîtes aux lettres et les facteurs de risque énumérés ci-dessus.

Utilisation de la validation de l'API avec le AWS CLI

Les exemples suivants vous montrent comment valider les adresses e-mail à l'aide du AWS CLI.

Pour valider une adresse e-mail à l'aide du AWS CLI

Vous pouvez utiliser l'[GetEmailAddressInsights](#) opération dans l'API Amazon SES v2 pour valider les adresses e-mail. Vous pouvez appeler cette opération à partir du AWS CLI, comme indiqué dans les exemples suivants.

- Validez une seule adresse e-mail :

```
aws --region us-east-1 sesv2 get-email-address-insights --email-address
user@example.com
```

- La réponse devrait ressembler à ceci :

```
{
  "MailboxValidation": {
    "IsValid": {
      "ConfidenceVerdict": "HIGH"
    },
    "Evaluations": {
      "HasValidSyntax": {
        "ConfidenceVerdict": "HIGH"
      },
      "HasValidDnsRecords": {
        "ConfidenceVerdict": "MEDIUM"
      },
      "MailboxExists": {
        "ConfidenceVerdict": "MEDIUM"
      },
      "IsRoleAddress": {
        "ConfidenceVerdict": "LOW"
      },
      "IsDisposable": {
        "ConfidenceVerdict": "LOW"
      },
      "IsRandomInput": {
        "ConfidenceVerdict": "LOW"
      }
    }
  }
}
```

- Pour plus d'informations sur les valeurs de réponse et les types de données, consultez le type de [MailboxValidation](#) données dans la référence de l'API Amazon SES v2.

- Assurez-vous que votre identité IAM dispose des autorisations requises pour les appels d'API de validation des e-mails et la publication CloudWatch des métriques :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EmailValidationPermissions",
      "Effect": "Allow",
      "Action": [
        "ses:GetEmailAddressInsights",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*"
    }
  ]
}
```

L'GetEmailAddressInsights autorisation est requise pour les appels de validation d'API et CreateServiceLinkedRole permet de publier CloudWatch des métriques pour les activités de validation.

Interprétation des résultats de validation

La réponse de validation inclut des verdicts de confiance pour vous aider à prendre des décisions concernant les adresses e-mail :

- **IsValid**— Évaluation de la validité globale avec un verdict de confiance élevé, moyen ou faible. Un niveau de fiabilité élevé indique une probabilité de livraison élevée pour l'adresse e-mail, un niveau MOYEN indique une probabilité de livraison modérée et un niveau faible indique une faible probabilité de livraison.
- **Evaluations**— Résultats d'évaluation individuels, chacun assorti d'un verdict de confiance :
 - **HIGH**— Indication forte de la vérification spécifique (par exemple, HIGH IsRandomInput signifie que l'e-mail est très probablement généré de manière aléatoire).
 - **MEDIUM**— Indication modérée de la vérification spécifique (par exemple, MEDIUM IsRandomInput signifie qu'il est probable que l'adresse e-mail soit générée de manière aléatoire).

- LOW— Indication faible ou inexistante de la vérification spécifique (par exemple, FAIBLE). `IsRandomInput` signifie que l'adresse e-mail est moins susceptible d'être générée de manière aléatoire).

Validation automatique

La validation automatique examine automatiquement toutes les adresses e-mail sortantes avant de les envoyer et ne distribue les messages qu'aux destinataires qui atteignent le seuil de validation que vous avez sélectionné. Cela vous aide à protéger votre réputation d'expéditeur en empêchant les envois vers des adresses probablement non valides ou risquées sans intervention manuelle ni intégration d'API.

Lorsque la validation automatique est activée, Amazon SES valide l'adresse de chaque destinataire dans le cadre de la tentative de livraison. Les adresses qui n'atteignent pas votre seuil sont automatiquement supprimées. Vous pouvez également configurer les [destinations des événements](#) pour savoir quels e-mails n'ont pas dépassé le seuil de validation.

Seuils de validation

La validation automatique prend actuellement en charge trois seuils de validation :

- Géré par SES — Amazon SES gère automatiquement le seuil de suppression des adresses non valides. Cette option permet à Amazon SES d'optimiser le seuil de validation en fonction de vos habitudes d'envoi et de votre réputation.
- Élevé — Permet d'envoyer des e-mails uniquement à des adresses présentant une probabilité de livraison élevée. Cela garantit une protection maximale de votre réputation d'expéditeur, mais peut supprimer certaines adresses légitimes dont le niveau de confiance en matière de livraison est moyen.
- Moyen — Permet d'envoyer des e-mails à des adresses dont la probabilité de livraison est moyenne ou élevée. Cela permet d'établir un équilibre entre la protection de la réputation et la portée des livraisons en autorisant les adresses présentant un niveau de confiance moyen ou élevé en matière de livraison. Cela supprime la livraison à des adresses e-mail peu fiables.

 Important

Si vous choisissez des seuils élevés ou moyens plutôt que des seuils gérés par SES, il est important de surveiller régulièrement vos indicateurs de livraison et vos résultats de validation.

Gestion de la validation automatique avec la console Amazon SES

La procédure suivante explique comment activer ou modifier les paramètres de validation automatique à l'aide de la console Amazon SES.

Pour gérer la validation automatique 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 volet de navigation de gauche, choisissez Validation automatique sous Validation par e-mail.
3. Cochez la case Activé pour activer la fonctionnalité.
4. Choisissez un seuil de validation.
5. Sélectionnez Enregistrer les modifications.

Le panneau de validation automatique affiche vos paramètres mis à jour.

 Important

La validation automatique s'applique à tous les e-mails sortants envoyés par le biais de votre compte. Les adresses qui n'atteignent pas votre seuil seront supprimées. Vous avez également la possibilité d'activer la validation automatique au niveau du jeu de configuration. Les envois supprimés sont toujours pris en compte dans votre quota d'envoi quotidien et les frais de message sortant standard pour les envois supprimés, en plus des frais de validation automatique, vous seront toujours facturés. Pour obtenir des informations sur la tarification, consultez la [page de tarification SES](#).

Activer la validation automatique au niveau de l'ensemble de configuration

Vous pouvez remplacer les paramètres de validation automatique au niveau du compte pour des ensembles de configuration spécifiques. Cela vous permet d'appliquer différents seuils de validation pour différents types de campagnes par e-mail.

Pour configurer la validation automatique pour un ensemble de configurations

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 Ensembles de configuration sous Configuration.
3. Choisissez le jeu de configuration que vous souhaitez configurer.
4. Dans la section Options de validation automatique, choisissez Modifier.
5. Cochez la case Annuler les paramètres de validation automatique au niveau du compte.
6. Cochez la case Validation automatique activée pour activer la validation automatique pour cet ensemble de configurations.
7. Pour le seuil de validation, sélectionnez l'une des options suivantes :
 - Géré par SES : Amazon SES gère automatiquement le seuil.
 - Élevé — Uniquement les adresses présentant une probabilité de livraison élevée.
 - Moyen — Adresses présentant une probabilité de livraison moyenne.
8. Sélectionnez Enregistrer les modifications.

Si vous ne remplacez pas les paramètres au niveau du compte, le jeu de configuration utilisera les paramètres de validation automatique définis au niveau du compte. Vous pouvez également configurer des [destinations d'événements](#) pour savoir quels e-mails n'ont pas dépassé le seuil de validation.

Gestion de la validation automatique à l'aide du AWS CLI

Les exemples suivants vous montrent comment activer et configurer la validation automatique à l'aide du AWS CLI.

Pour gérer la validation automatique à l'aide du AWS CLI

Vous pouvez utiliser l'[PutAccountSuppressionAttributes](#) opération dans l'API Amazon SES v2 pour gérer la validation automatique. Vous pouvez appeler cette opération à partir du AWS CLI, comme indiqué dans les exemples suivants.

- Activez la validation automatique avec un seuil élevé :

```
aws --region us-east-1 sesv2 put-account-suppression-attributes --cli-input-json
file://auto-validation.json
```

Le fichier d'entrée ressemble à ceci :

```
{
  "SuppressedReasons": ["BOUNCE", "COMPLAINT"],
  "ValidationOptions": {
    "ConditionThreshold": {
      "ConditionThresholdEnabled": "ENABLED",
      "OverallConfidenceThreshold": {
        "Verdict": "HIGH"
      }
    }
  }
}
```

- Définissez le seuil sur « moyen » :

```
{
  "SuppressedReasons": ["BOUNCE", "COMPLAINT"],
  "ValidationOptions": {
    "ConditionThreshold": {
      "ConditionThresholdEnabled": "ENABLED",
      "OverallConfidenceThreshold": {
        "Verdict": "MEDIUM"
      }
    }
  }
}
```

- Utilisez le seuil géré par SES :

```
{
  "SuppressedReasons": ["BOUNCE", "COMPLAINT"],
  "ValidationOptions": {
```

```

        "ConditionThreshold": {
            "ConditionThresholdEnabled": "ENABLED",
            "OverallConfidenceThreshold": {
                "Verdict": "MANAGED"
            }
        }
    }
}

```

- Désactiver la validation automatique :

```

{
    "SuppressedReasons": ["BOUNCE", "COMPLAINT"],
    "ValidationOptions": {
        "ConditionThreshold": {
            "ConditionThresholdEnabled": "DISABLED"
        }
    }
}

```

- Pour vérifier le résultat :

```
aws --region us-east-1 sesv2 get-account
```

Pour plus d'informations sur les valeurs des paramètres et les types de données, consultez le type de [SuppressionAttributes](#) données dans la référence de l'API Amazon SES v2.

Pour configurer la validation automatique pour un ensemble de configuration à l'aide du AWS CLI

Vous pouvez utiliser cette [PutConfigurationSetSuppressionOptions](#) opération pour remplacer les paramètres de validation automatique d'un ensemble de configuration spécifique.

- Remplacez les paramètres au niveau du compte pour un ensemble de configuration :

```
aws --region us-east-1 sesv2 put-configuration-set-suppression-options --cli-input-
json file://config-set-auto-validation.json
```

Le fichier d'entrée ressemble à ceci :

```

{
    "ConfigurationSetName": "my-config-set",

```

```
"SuppressedReasons": ["BOUNCE", "COMPLAINT"],
"ValidationOptions": {
  "ConditionThreshold": {
    "ConditionThresholdEnabled": "ENABLED",
    "OverallConfidenceThreshold": {
      "Verdict": "HIGH"
    }
  }
}
```

- Pour vérifier le résultat :

```
aws --region us-east-1 sesv2 get-configuration-set --configuration-set-name my-
config-set
```

Tableau de bord de validation des e-mails

Le tableau de bord de validation des e-mails fournit une visibilité sur votre activité de validation des e-mails, en affichant les résultats de validation classés par niveau de confiance en termes de probabilité de livraison. Vous pouvez surveiller les tendances de validation pour les validations d'API et les validations de console afin de comprendre la qualité de vos listes d'e-mails et de prendre des décisions éclairées concernant vos pratiques d'envoi.

Accès au tableau de bord

Pour consulter le tableau de bord de validation des e-mails :

1. Connectez-vous à la console Amazon SES à l'adresse <https://console.aws.amazon.com/ses/>.
2. Dans le volet de navigation, choisissez Email Validation.
3. Choisissez l'élément de menu Tableau de bord de validation des e-mails pour afficher les métriques de validation.

Le tableau de bord fournit une représentation visuelle de votre activité de validation, vous aidant à identifier les tendances et à prendre des décisions basées sur les données concernant l'hygiène des listes et les pratiques d'envoi.

Email validation dashboard

Email validation metrics for US East (N. Virginia)

Date range

Last 7 days

Email validation results counts

The following metrics show total volumes of validation confidence levels for the date range selected.

Low

8,026

Medium

8,322

High

8,757

Email validation results trends

High validity confidence indicates high delivery likelihood for the email address, medium indicates moderate delivery likelihood and low indicates low delivery likelihood. This metric is emitted when the GetEmailAddressInsights API is called or the Email addresses validation page is used.

Volume

Low Medium High

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. Consultez [the section called “Prise en main”](#).

Rubriques

- [Commencer à utiliser Mail Manager](#)
- [Points de terminaison d'entrée](#)
- [Politiques de circulation et déclarations de politique](#)
- [Ensembles de règles et règles](#)
- [relais SMTP](#)
- [Listes d'adresses](#)
- [Archivage des e-mails](#)
- [Compléments par e-mail](#)
- [Politiques d'autorisation pour Mail Manager](#)
- [Journalisation du gestionnaire de courrier](#)

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, consultez [the 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, consultez [the 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, consultez [the 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 à chacun d'entre eux la gestion et le routage de 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 en savoir plus, 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 en savoir plus, 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 dans [the section called “Configuration du point de terminaison public”](#).

Configuration de votre environnement pour utiliser un point de terminaison d'entrée

SES prend en charge à la fois les points de terminaison publics et les points de terminaison Amazon Virtual Private Cloud (VPC) pour que les points de terminaison d'entrée acceptent les e-mails entrants. Les sections suivantes expliquent comment configurer votre point de terminaison d'entrée pour utiliser l'une de ces options.

Rubriques

- [Réception d'e-mails via les points de terminaison publics](#)
- [Réception d'e-mails via les points de terminaison Amazon VPC](#)

Réception d'e-mails via les points de terminaison publics

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.
- Port pris en charge : 25
- Supporte STARTTLS : Oui
- 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.
 - Ports pris en charge : 25, 587 ([RFC 2476](#))
 - Supporte STARTTLS : Oui
- Point de terminaison mTLS : le courrier envoyé à votre domaine doit provenir de clients présentant un certificat client TLS signé par l'une des autorités de certification (CA) du trust store du point de terminaison d'entrée. Consultez [the section called "Authentication mTLS"](#).
 - Copiez et collez la valeur de l'enregistrement « A » directement dans la configuration SMTP d'un client SMTP sur site.
 - Port pris en charge : 25
 - Supporte STARTTLS : Oui

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`

Connexion au point de terminaison authentifié

Pour les expéditeurs autorisés avec lesquels vous avez partagé vos informations d'identification SMTP afin de vous connecter à votre point de terminaison authentifié, les protocoles suivants doivent être suivis pour le nom d'utilisateur et le mot de passe afin d'établir une connexion réussie avec le serveur :

- Nom d'utilisateur — Il s'agit de l'ID du point de terminaison d'entrée qui doit être codé en Base64. (Voir [l'étape 11](#) dans les procédures de la console pour savoir comment trouver l'ID du point de terminaison d'entrée.)
- Mot de passe : il s'agit de celui utilisé lors de la création du point de terminaison d'entrée et doit être encodé en Base64.

L'exemple suivant montre un serveur AUTH SMTP typique et un échange de clients établissant une connexion :

```
S: 250 AUTH LOGIN PLAIN
C: AUTH LOGIN
S: 334 VXN1cm5hbWU6
C: SW5ncmVzc1BvaW50
S: 334 UGFzc3dvcmQ6
C: SW5ncmVzc1Bhc3N3b3Jk
S: 235 Authentication successful
```

Cet exemple contient les propriétés suivantes :

- Ssignifie « serveur » : le serveur SMTP qui accepte les messages.
- Csignifie « client » : le client SMTP établit une connexion avec le serveur et envoie des messages au serveur.
- 250 AUTH LOGIN PLAINest une réponse du serveur avec les méthodes AUTH prises en chargeAUTH PLAIN, AUTH LOGIN ou l'expéditeur peut choisir l'une d'entre elles et envoyer des commandes SMTP conformes à la spécification d'extension de service SMTP pour l'authentification RFC 2554. AUTH LOGINest utilisé ici.
- 334 VXN1cm5hbWU6— Le serveur demande le nom d'utilisateur en Base64.
- SW5ncmVzc1BvaW50— Le client répond avec l'ID du point de terminaison d'entrée en Base64.
- 334 UGFzc3dvcmQ6— Le serveur demande le mot de passe en Base64.

- SW5ncmVzc1Bhc3N3b3Jk— Le client répond avec le mot de passe du point de terminaison d'entrée en Base64.

Réception d'e-mails via les points de terminaison Amazon VPC

Outre les points de terminaison d'entrée publics, vous pouvez utiliser des points de terminaison VPC avec des points de terminaison d'entrée SES pour une ingestion sécurisée et privée des e-mails au sein de votre infrastructure réseau privée.

Différences de configuration par rapport à l'utilisation de points de terminaison d'entrée publics

- L'enregistrement « A » généralement disponible pour les terminaux publics n'est pas fourni.
- Vous devez vous connecter au point de terminaison d'entrée à l'aide des noms DNS fournis par votre point de terminaison VPC.
- Toutes les connexions utilisent un réseau privé au sein de votre VPC.

Types de points de terminaison d'entrée pris en charge via les points de terminaison VPC

SES prend en charge deux types de points d'entrée via les points de terminaison VPC :

- Point de terminaison d'entrée ouvert : les e-mails envoyés à votre domaine sont acheminés directement via le point de terminaison VPC sans nécessiter d'authentification de l'expéditeur.

Exigences de configuration :

- Créez un point de terminaison d'entrée ouvert privé en l'associant à un ID de point de terminaison VPC que vous possédez.
- Ports pris en charge : 25, 587
- Supporte STARTTLS : Oui
- Point de terminaison d'entrée 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.

Exigences de configuration :

- Créez un point de terminaison d'entrée authentifié privé en l'associant à un ID de point de terminaison VPC que vous possédez.
- Ports pris en charge : 25, 587

- Supporte STARTTLS : Oui
- L'authentification utilise le même mécanisme de nom d'utilisateur et de mot de passe codés en base64 que les points de terminaison authentifiés publics.
- Point de terminaison d'entrée mTLS : le courrier envoyé à votre domaine doit provenir de clients présentant un certificat client TLS signé par l'une des autorités de certification dans le trust store du point de terminaison d'entrée. Consultez [the section called “Authentication mTLS”](#).

Exigences de configuration :

- Créez un point de terminaison d'entrée mTLS privé en l'associant à un identifiant de point de terminaison VPC que vous possédez.
- Ports pris en charge : 25, 587
- Supporte STARTTLS : Oui

Exigences relatives aux points de terminaison VPC

Pour utiliser un point de terminaison VPC avec un point de terminaison d'entrée SES, les conditions suivantes doivent être remplies :

- Le point de terminaison du VPC doit être actif et disponible.
- Le point de terminaison VPC doit appartenir au même AWS compte que le point de terminaison d'entrée (l'accès entre comptes n'est pas pris en charge).
- Le point de terminaison VPC doit être créé pour le nom de service approprié en fonction du type de point de terminaison d'entrée :
 - Point de terminaison d'entrée ouvert — `com.amazonaws.region.mail-manager-smtp.open`
 - Point de terminaison d'entrée authentifié — `com.amazonaws.region.mail-manager-smtp.auth`
 - Point de terminaison d'entrée mTLS — `com.amazonaws.region.mail-manager-smtp.mtls`
 - Point de terminaison d'entrée ouvert FIPS — `com.amazonaws.region.mail-manager-smtp.open.fips`
 - Point de terminaison d'entrée authentifié FIPS — `com.amazonaws.region.mail-manager-smtp.auth.fips`

- Point de terminaison d'entrée FIPS mTLS — `com.amazonaws.region.mail-manager-smtp.mtls.fips`

Remarques de configuration importantes

- One-to-one relation — Chaque point de terminaison VPC ne peut être associé qu'à un seul point de terminaison d'entrée. Vous ne pouvez pas utiliser le même point de terminaison VPC pour plusieurs points de terminaison d'entrée.
- Aucune politique de point de terminaison VPC : contrairement aux autres AWS services, les points de terminaison VPC utilisés avec des points de terminaison d'entrée ne prennent pas en charge les politiques de point de terminaison VPC. SES vérifie automatiquement que le propriétaire du point de terminaison VPC et le propriétaire du point de terminaison d'entrée sont le même compte. AWS
- DNS privé uniquement : tous les noms DNS fournis par le point de terminaison du VPC seront des noms DNS privés accessibles uniquement au sein de votre VPC.
- Validation au moment de la création : SES effectue la validation lors de la création des ressources pour s'assurer que le point de terminaison du VPC répond à toutes les exigences.
- La politique TLS doit correspondre au service de point de terminaison VPC : lors de la création d'un point de terminaison d'entrée privé, la valeur de la politique TLS doit correspondre au type de service de point de terminaison VPC. Un point de terminaison d'entrée doté d'une politique FIPS TLS doit utiliser un service de point de terminaison VPC FIPS, et un point de terminaison d'entrée doté d'une politique TLS doit utiliser REQUIRED un OPTIONAL service de point de terminaison VPC non FIPS. Ils ne peuvent pas être mélangés.

Connexion à votre point de terminaison d'entrée via un point de terminaison VPC

Après avoir configuré votre point de terminaison VPC et votre point de terminaison d'entrée :

1. Récupérez les noms DNS générés pour votre point de terminaison VPC.
2. Configurez vos clients SMTP ou vos serveurs de messagerie pour utiliser ces noms DNS pour la connexion.
3. Si vous utilisez un point de terminaison authentifié, configurez vos clients SMTP avec les informations d'identification codées en base64 appropriées utilisées avec votre point de terminaison d'entrée authentifié.

Rotation des informations d'identification SMTP pour les points de terminaison d'entrée authentifiés

Lorsque vous utilisez un point de terminaison d'entrée authentifié, vous devrez peut-être changer régulièrement le mot de passe SMTP utilisé par vos clients d'envoi. Le comportement de rotation dépend de la manière dont vous stockez vos informations d'identification : en utilisant AWS Secrets Manager ou en utilisant le stockage géré par SES.

AWS Secrets Manager stockage de mots de passe basé

Si vous avez configuré votre point de terminaison d'entrée authentifié avec un secret stocké dans AWS Secrets Manager, Mail Manager utilise la `AWSCURRENT` version du secret pour l'authentification et accepte également cette version. `AWSPREVIOUS` Cela signifie que les anciens et les nouveaux mots de passe sont valides pendant et après la rotation, ce qui donne à vos clients expéditeurs le temps de mettre à jour leurs informations d'identification.

La `AWSPREVIOUS` version n'expire pas du côté du gestionnaire de courrier : elle reste valide tant qu'elle existe dans AWS Secrets Manager. Il est de votre responsabilité de gérer les versions secrètes et leur date d'expiration AWS Secrets Manager.

Pour configurer la rotation automatique :

1. Configurez [la rotation automatique](#) sur votre secret in AWS Secrets Manager.
2. En cas de rotation, AWS Secrets Manager déplace l'`AWSCURRENT` étiquette vers la nouvelle version secrète et l'attache `AWSPREVIOUS` à l'ancienne version actuelle.
3. Mail Manager accepte immédiatement les deux versions, de sorte que les clients expéditeurs peuvent mettre à jour leurs informations d'identification sans interruption.

Pour plus d'informations sur les stratégies AWS Secrets Manager de rotation, consultez la section [Secrets de rotation](#) dans le guide de AWS Secrets Manager l'utilisateur.

Stockage de mots de passe géré par SES

Si vous définissez le mot de passe directement lors de la création du point de terminaison d'entrée (ou si vous le mettez à jour à l'aide de l'`UpdateIngressPointAPI`), Mail Manager prend en charge le mot de passe précédent pendant 14 jours après la mise à jour. Après 14 jours, les clients qui envoient des messages en utilisant l'ancien mot de passe reçoivent `Authentication failed` des erreurs.

Coordination de la rotation avec les clients d'origine

Lorsque vous planifiez une rotation des identifiants, prévenez à l'avance les propriétaires de vos applications d'envoi et assurez-vous qu'ils mettent à jour leurs configurations SMTP dans le délai de grâce. Pour le stockage AWS Secrets Manager basé, le délai de grâce dure aussi longtemps que la AWSPREVIOUS version existe. Pour le stockage géré par SES, le délai de grâce est de 14 jours.

Note

Pour une rotation fluide des informations d'identification avec un minimum de perturbations pour le client, utilisez un stockage de mots de passe AWS Secrets Manager basé sur lequel la rotation automatique est configurée.

Politique TLS pour les points de terminaison d'entrée

La politique TLS d'un point de terminaison d'entrée détermine si les clients SMTP connectés doivent utiliser le cryptage TLS lors de l'envoi d'e-mails à votre point de terminaison. Vous pouvez spécifier une politique TLS lors de la création d'un point de terminaison d'entrée à l'aide de l'CreateIngressPointAPI, et la modifier ultérieurement à l'aide de l'UpdateIngressPointAPI. La politique TLS par défaut dépend de votre région : FIPS c'est la politique par défaut dans les régions des États-Unis et du Canada, et REQUIRED c'est celle par défaut dans toutes les autres régions.

Toutes les connexions aux points de terminaison d'entrée utilisent le protocole TLS opportuniste via la commande STARTTLS. La connexion commence en texte brut et est mise à niveau vers le protocole TLS si le client de connexion le prend en charge. Le protocole TLS implicite (TLS Wrapper), dans lequel la connexion démarre chiffrée, n'est pas pris en charge.

Les valeurs de politique TLS suivantes sont disponibles :

- **FIPS** — Nécessite le chiffrement TLS à l'aide de modules FIPS-validated cryptographiques. Il s'agit de la valeur par défaut dans les régions des États-Unis et du Canada et n'est disponible que dans ces régions.
- **OBLIGATOIRE** — Les clients SMTP connectés doivent utiliser le cryptage TLS. Les connexions qui n'utilisent pas le protocole TLS sont rejetées. Il s'agit de la valeur par défaut dans les régions autres que les États-Unis et le Canada.
- **FACULTATIF** — Le chiffrement TLS est pris en charge mais n'est pas obligatoire. Les clients SMTP connectés peuvent envoyer des e-mails avec ou sans TLS.

Disponibilité par type de point de terminaison d'entrée

Les valeurs de politique TLS ne sont pas toutes valides pour chaque combinaison de type de point de terminaison d'entrée et de configuration réseau :

- **FIPS** — Peut être utilisé avec tous les types de terminaux d'entrée (ouverts, authentifiés et MTL) sur les réseaux publics et privés, mais uniquement dans les régions des États-Unis et du Canada. Une fois défini, il FIPS ne peut pas être remplacé par une autre valeur par le biais d'une mise à jour. Si vous avez besoin d'une politique TLS différente, vous devez créer un nouveau point de terminaison d'entrée.
- **OBLIGATOIRE** — Peut être utilisé avec tous les types de terminaux d'entrée dans toutes les régions. Toutefois, pour les points de terminaison authentifiés et d'entrée MTL sur les réseaux publics, ils ne peuvent être définis qu'au moment de la création ; ils ne **REQUIRED** peuvent pas être modifiés par le biais d'une mise à jour. Pour les points de terminaison d'entrée ouverts (publics ou privés) et les points de terminaison d'entrée authentifiés ou MTL sur les réseaux privés, ils **REQUIRED** peuvent être définis au moment de la création et modifiés par le biais d'une mise à jour. Notez que ce **nREQUIRED** est pas disponible pour les points de terminaison authentifiés ou d'entrée mTLS sur les réseaux publics dans les régions des États-Unis et du Canada, où il FIPS est utilisé à la place.
- **FACULTATIF** — Peut être utilisé avec des points de terminaison d'entrée ouverts sur les réseaux publics et privés, et avec des points de terminaison d'entrée authentifiés sur des réseaux privés. **OPTIONAL** n'est pas disponible pour les points de terminaison d'entrée mTLS et n'est pas disponible pour les points de terminaison d'entrée authentifiés sur les réseaux publics.

Règles de modification de la politique TLS

Les règles suivantes s'appliquent lors de la mise à jour de la politique TLS sur un point de terminaison d'entrée existant :

- FIPS ne peut pas être modifié après la création.
- Pour les points de terminaison d'entrée ouverts et les points de terminaison d'entrée authentifiés sur les réseaux privés, vous pouvez basculer entre **et. REQUIRED** **OPTIONAL**
- Pour les points de terminaison d'entrée MTL et les points de terminaison d'entrée authentifiés sur les réseaux publics, la politique TLS ne peut pas être modifiée après sa création.

Authentification TLS mutuelle (mTLS) pour les points de terminaison d'entrée

L'authentification TLS mutuelle (mTLS) nécessite de connecter les clients SMTP pour présenter un certificat client TLS signé par l'une des autorités de certification (CA) dans la banque de confiance du point de terminaison d'entrée. Seuls les clients possédant des certificats fiables peuvent envoyer des e-mails à votre terminal.

Pour créer un point de terminaison d'entrée mTLS, choisissez-le comme type de point de terminaison d'entrée et fournissez un `TlsAuthConfiguration` contenant `TrustStore` dans le `IngressPointConfiguration` paramètre de l'API. `CreateIngressPoint`

Configuration du Trust Store

Le trust store définit les certificats clients acceptés par votre point de terminaison d'entrée. Il contient les champs suivants :

- `CAcontent` (obligatoire) — Un ensemble de certificats d'autorité de certification (CA) au format PEM. Ce bundle contient les certificats CA utilisés pour valider les certificats clients. Vous pouvez inclure plusieurs certificats CA dans un seul ensemble, jusqu'à 500 Ko.
- `CrlContent`(facultatif) — Une liste de révocation de certificats (CRL) au format PEM. S'ils sont fournis, les certificats clients qui apparaissent sur la CRL sont rejetés même s'ils sont signés par une autorité de certification approuvée. Jusqu'à 500 Ko.
- `KmsKeyArn`(facultatif) — L'ARN d'une clé gérée par le AWS KMS client (CMK) utilisée pour chiffrer les données du trust store. Si elle n'est pas spécifiée, une clé AWS gérée est utilisée. Lorsque vous utilisez une clé CMK, la politique de clé doit autoriser SES à utiliser la clé. Consultez [Politique de clé gérée par le client \(CMK\) de KMS pour le magasin de confiance de MTL](#).

Les certificats expirés sont considérés comme non valides et ne sont pas acceptés dans les connexions. SES filtre également les certificats CA expirés et les listes de révocation de certificats expirés (CRL) de votre magasin de confiance. Si une CRL expire, le certificat CA associé à cette CRL est également supprimé du trust store, ce qui signifie que les clients signés par cette autorité de certification ne pourront plus se connecter tant que vous n'aurez pas fourni une CRL mise à jour.

Utilisation des attributs du certificat client dans les conditions des règles

Lorsqu'un client se connecte à un point de terminaison d'entrée mTLS avec un certificat valide, les attributs du certificat (tels que les champs Nom commun, numéro de série et nom alternatif du sujet)

sont mis à disposition pour être utilisés dans les conditions de règle sous forme d'expressions de chaîne. Cela vous permet d'acheminer, de filtrer ou d'agir sur le courrier électronique en fonction de l'identité du client qui se connecte. Pour obtenir la liste complète des attributs disponibles, consultez la référence relative [aux conditions des règles](#).

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, authentifié ou mTLS.
 - Si vous choisissez Authentifié, sélectionnez soit un mot de passe SMTP et saisissez-en un (à partager avec les expéditeurs autorisés), 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.
 - Si vous choisissez mTLS, vous devez fournir une configuration Trust Store contenant votre bundle de certificats CA. Facultativement, vous pouvez également fournir une liste de révocation de certificats et une AWS KMS clé. Consultez [the section called “Authentication mTLS”](#).
 - 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. Par Key/value paire, 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 un ensemble de règles contenant les actions de règles que vous souhaitez effectuer sur l'e-mail que vous autorisez à entrer.
7. Sélectionnez une politique de trafic pour déterminer l'e-mail que vous souhaitez bloquer ou autoriser.
8. Choisissez s'il s'agit d'un réseau public ou privé.
 - Pour un réseau public, choisissez l'adressage IPv4 uniquement ou Dualstack (IPv4 et IPv6).
 - Pour un réseau privé, sélectionnez ou entrez un point de terminaison VPC que vous avez partagé avec des expéditeurs autorisés dans le même compte, tels que des utilisateurs ou des rôles IAM. Vous pouvez éventuellement créer un nouveau point de terminaison VPC en choisissant Create VPC endpoint pour ouvrir la console Amazon VPC.
9. Sélectionnez une politique TLS pour votre point de terminaison d'entrée. La valeur par défaut dépend de votre région. Consultez [Politique TLS](#) pour plus de détails sur les valeurs disponibles et les restrictions.
10. Sélectionnez Créer un point de terminaison d'entrée.
11. 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 dans [Configuration du point de terminaison public](#).
12. Juste au-dessus du conteneur Informations générales de la console, se trouve un grand numéro non étiqueté préfixé par « inp » (également reproduit dans le fil d'Ariane en haut de la page), par exemple, inp-1abc2de3fghi4jkl5mnop6qr. C'est ce que l'on appelle l'ID du point de terminaison d'entrée. Sa valeur est utilisée comme nom d'utilisateur pour vous connecter à votre serveur d'entrée. (Vous devrez le partager avec vos expéditeurs autorisés pour vous connecter à votre terminal.)
13. 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.
14. Pour modifier un point de terminaison d'entrée, sélectionnez son nom pour ouvrir sa page de résumé :

- Vous pouvez modifier l'état actif ou la politique TLS du point de terminaison (pour les configurations prises en charge) en choisissant Modifier dans 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 supprimé. Vous pouvez également définir l'action par défaut de la politique pour autoriser ou bloquer les e-mails non conformes aux conditions de vos déclarations de politique. Il s'agit d'une action « catch all » pour la politique de trafic.

Les déclarations de politique sont également créées avec une action d'autorisation ou de blocage prise lorsque les conditions des déclarations sont remplies. Vous créez les conditions en sélectionnant une propriété d'e-mail 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 :

- 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.
- Taille maximale des messages — Si ce paramètre facultatif est défini, tout message supérieur à cette taille est supprimé.

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 une propriété d'e-mail 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 d'e-mail](#), vous pourrez le sélectionner ici en tant que propriété d'e-mail.
 - Les politiques de trafic associées aux points de terminaison d'entrée à double pile IPv6 ou à double pile n'évalueront ni n'appliqueront les conditions d'ajout de courrier électronique aux messages reçus par le biais de connexions. IPv6 Les conditions d'ajout d'e-mail ne s'appliqueront qu'aux messages reçus via des IPv4 connexions sur des points de terminaison à double pile.
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 allow/deny propriété 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 toutes les propriétés de déclaration de stratégie disponibles pour créer une condition de déclaration de stratégie. 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 de la déclaration de politique : propriétés, opérateurs et valeurs

Propriété	Type d'expression
Adresse du destinataire	
Abusix Mail Intelligence (si vous êtes abonné)	
• Répertorié sur	Opérateurs et valeurs valides pour les expressions de chaîne
Liste de domaines bloqués Spamhaus (si abonné)	
• Répertorié sur	
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
Abusix Mail Intelligence (si vous êtes abonné)	
• Est listé	Opérateurs et valeurs valides pour les expressions booléennes
Liste de domaines bloqués Spamhaus (si abonné)	

Propriété	Type d'expression
• Est listé	

Correspondance et sous-adressage des adresses des destinataires

La propriété d'adresse du destinataire utilise l'adresse complète du destinataire de l'enveloppe SMTP exactement telle qu'elle a été reçue, y compris toute extension de sous-adresse (également appelée « adressage plus »). Par exemple, si un message est envoyé à `user+tag@example.com`, l'adresse du destinataire évaluée dans la déclaration de politique ne l'est `user+tag@example.com` pas `user@example.com`.

Cela signifie que le ciblage d'une CONTAINS règle EQUALS ou ne `user@example.com` correspondra pas `user+tag@example.com`. Si vous devez faire correspondre toutes les variantes sous-adressées d'une adresse, pensez à utiliser une liste d'adresses contenant des caractères génériques (par exemple, `user*@example.com`). Vous pouvez également utiliser le domaine (par exemple, `@example.com`) pour une correspondance plus large au niveau du domaine. ENDS_WITH

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, sans exception.

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 explique 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, les and/or exceptions ne le sont pas. Pour ajouter d'autres actions à effectuer, sélectionnez Ajouter une nouvelle action. Lorsque vous créez deux actions ou plus, up/down des flèches s'affichent pour vous permettre de définir l'ordre d'exécution.

Note

Pour exécuter l'une de ces [actions de règle](#), vous devez activer leur politique d'autorisation respective pour votre compte ; sinon, l'action de règle échouera.

9. Appliquez la politique d'autorisation pour chacune de ces actions directement depuis le panneau des détails de la règle après avoir sélectionné l'action :
 - a. Choisissez Créer un nouveau rôle dans le champ Rôle IAM et entrez un nom suivi de Créer un rôle. (La politique de confiance IAM pour ce rôle sera automatiquement générée en arrière-plan.)
 - b. Comme la politique de confiance IAM a été générée automatiquement, il vous suffit d'ajouter la politique d'autorisation de l'action au rôle. Sélectionnez Afficher le rôle dans le champ Rôle IAM pour ouvrir la console IAM.
 - c. Sous l'onglet Autorisations, choisissez Ajouter des autorisations et sélectionnez Créer une politique intégrée.
 - d. Sur la page Spécifier les autorisations, sélectionnez JSON dans l'éditeur de politiques.
 - e. Copiez et collez la politique correspondante [Politiques d'autorisation pour Mail Manager](#) dans l'éditeur de politiques et remplacez les données en texte rouge par les vôtres. (Assurez-vous de supprimer tout exemple de code dans l'éditeur.)
 - f. Choisissez Suivant.
 - g. Passez en revue et créez votre politique d'autorisation pour le rôle IAM en choisissant Créer une politique.
 - h. Sélectionnez l'onglet de votre navigateur où la page de modification des règles de SES Mail Manager est ouverte et poursuivez les étapes restantes pour créer des règles.
10. 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 l'ensemble de règles situé dans le panneau Modifier l'ensemble de règles sur la gauche.
11. 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, up/down des flèches apparaissent dans la colonne Réorganisation de l'ensemble de règles afin que vous puissiez définir l'ordre d'exécution.
12. 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.
13. 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.

14. 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.
15. 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	
En-tête MIME	

Propriété	Type d'expression
Attribut de certificat client (points de terminaison d'entrée mTLS uniquement) • Numéro de série • Nom commun • Country • Locality • Organisation • Unité organisationnelle • State • Nom alternatif du sujet Vade Advanced Email Security (si vous êtes abonné) • Catégorie • Verdict Analyse antivirus Trend Micro (si vous êtes abonné) • Catégorie	
plage IP	Opérateurs et valeurs valides pour les expressions IP
Taille maximale du message	Opérateurs et valeurs valides pour les expressions numériques
DKIM	Opérateurs et valeurs valides pour les expressions de verdict
SPF	

Propriété	Type d'expression
TLS	Opérateurs et valeurs valides pour les expressions booléennes
Enveloppé en TLS	
Lire le reçu	
Vade Advanced Email Security (si vous êtes abonné)	
Est passé	Opérateurs et valeurs valides pour les expressions DMARC
Analyse antivirus Trend Micro (si vous êtes abonné) Est passé	
Politique du DMARC	

Correspondance et sous-adressage des adresses des destinataires

La propriété d'adresse du destinataire utilise l'adresse complète du destinataire de l'enveloppe SMTP exactement telle qu'elle a été reçue, y compris toute extension de sous-adresse (également appelée « adressage plus »). Par exemple, si un message est envoyé à `user+tag@example.com`, l'adresse du destinataire évaluée dans la condition de règle est `user+tag@example.com` « Non `user@example.com` ».

Cela signifie que le ciblage d'une CONTAINS règle EQUALS ou ne `user@example.com` correspondra pas `user+tag@example.com`. Si vous devez faire correspondre toutes les variantes sous-adressées d'une adresse, pensez à utiliser une liste d'adresses contenant des caractères génériques (par exemple, `user*@example.com`). Vous pouvez également utiliser le domaine (par exemple, `@example.com`) pour une correspondance plus large au niveau du domaine. ENDS_WITH

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.
relais SMTP	Relaie le courrier électronique via SMTP vers un autre serveur SMTP spécifique.
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 WorkMail boîte aux lettres	Envoie l'e-mail dans une WorkMail boîte aux lettres Amazon.

Les actions et leurs paramètres	Description
Livrer à Q Business	Envoie un e-mail à une application Amazon Q Business pour intégration dans sa base de connaissances.
Publier sur SNS	Publie le contenu de l'e-mail dans une rubrique Amazon SNS.
Envoyer vers Internet	Utilise SES pour envoyer l'e-mail au (x) destinataire (s) figurant sur la liste des destinataires de l'e-mail.
Rebondir	Fait rebondir l'e-mail en renvoyant une réponse de rebond à l'expéditeur.
Invoquer la fonction Lambda	Invoke une AWS Lambda fonction pour traiter l'e-mail. Le format de charge utile Lambda est identique à celui d'Amazon SES Email Receiving, comme décrit dans. Contenu des notifications Pour de plus amples informations, veuillez consulter Exemples de cas d'utilisation . Pour des exemples de code, consultez Exemples de fonctions Lambda .
Lâchez	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

 Note

Tous les points de terminaison SMTP que vous configurez avec le relais SMTP Amazon SES doivent être publics car les points de terminaison SMTP privés ne sont pas pris en charge.

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](#)

 Note

Assurez-vous que les destinations de vos destinataires sont des identités e-mail vérifiées par SES. Par exemple, si vous souhaitez envoyer des e-mails aux destinataires `abc@example.com`, `admin@example.com`, `postmaster@acme.com` et `support@acme.com`, nous vous recommandons de vérifier les `acme.com` domaines `example.com` et dans SES. Si la destination du destinataire n'est pas vérifiée, SES ne tentera pas de remettre l'e-mail au serveur SMTP public.

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 public 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 les valeurs suivantes Key/value par paires :

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 de relais SMTP SES Create 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.

Conditions préalables

- 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 :

Inbound gateway

If you use email gateways to route incoming email, please enter them here to improve spam handling [Learn more](#)

☒ Enable

1. Gateway IPs

IP addresses / ranges
34.234.65.103
76.223.191.89
206.55.128.0/24

[ADD](#)

☒ Automatically detect external IP (recommended)

☐ Reject all mail not from gateway IPs

☒ Require TLS for connections from the email gateways listed above

2. Message Tagging

☐ Message is considered spam if the following header regexp matches

Most changes take effect in a few minutes. [Learn more](#)
You can view prior changes in the [Audit log](#)

1 unsaved change CANCEL SAVE

- Dans IP de passerelle, sélectionnez Ajouter, puis ajoutez les adresses IP des points de terminaison d'entrée spécifiques à votre région dans le tableau des [plages d'adresses IP des relais SMTP](#).
- 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.

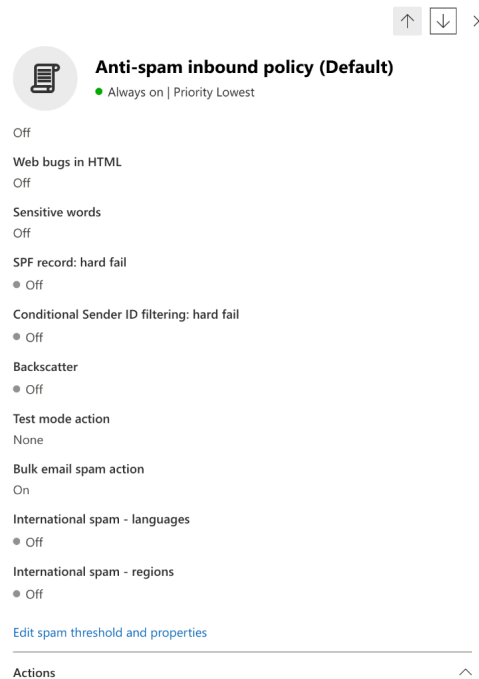
Conditions préalables

- Accès au centre d'administration Microsoft Security (centre d'[administration Microsoft Security > Courriel](#) 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 Anti-spamsous 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 des [plages d'adresses IP des relais SMTP](#).

- Cliquez sur Enregistrer.
- d. Revenez à l'Anti-spamoption et choisissez la politique Anti-spam d'entrée.
- Au bas de la boîte de dialogue, sélectionnez Modifier le seuil de spam et les propriétés :



- Faites défiler l'écran jusqu'à Marquer comme spam et assurez-vous que l'option SPF record : hard fail est définie sur Désactivé.
- Cliquez sur Enregistrer.

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

Add a connector

☒ New connector
☐ Name
☐ Authenticating sent email
☐ Security restrictions
☐ Review connector

Connector name

This connector allows your partner organization or service provider to send messages to Office 365 securely.

Name *

Simple Email Service MailManager connector

Description

Connector for filtering

What do you want to do after connector is saved?

☒ Turn it on

- 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 d'entrée spécifiques à votre région dans le tableau des plages d'adresses [IP des relais SMTP](#).

Add a connector

☒ New connector
☒ Name
☒ Authenticating sent email
☐ Security restrictions
☐ Review connector

Authenticating sent email

How do you want Office 365 to identify your partner organization?

Office 365 will only accept messages through this connector if your partner organization can be identified through one of the following two ways.

☐ By verifying that the sender domain matches one of the following domains
☒ By verifying that the IP address of the sending server matches one of the following IP addresses, which belong to your partner organization

Example: 10.5.3.2 or 10.3.1.5/24

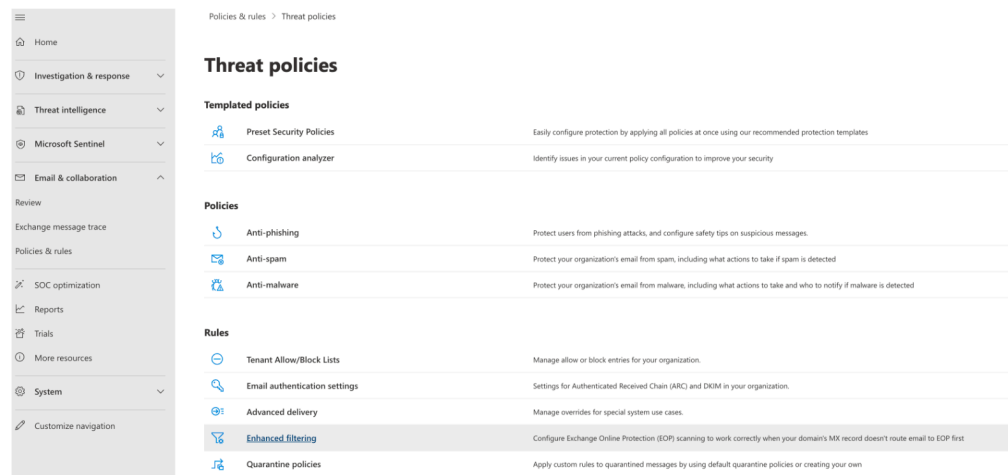
206.55.128.0/24

- 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.

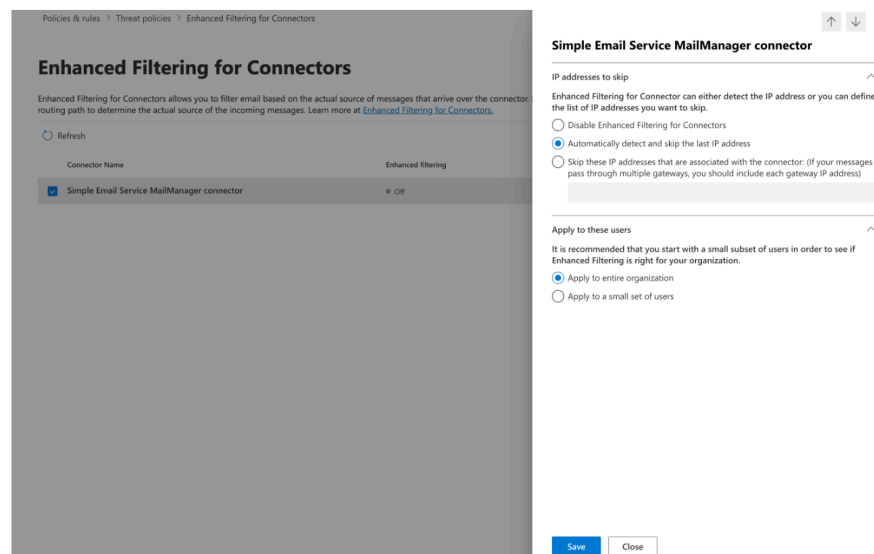
b. Activer le filtrage amélioré

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.



- Cliquez sur Enregistrer.

Listes d'adresses

Les listes d'adresses sont une fonctionnalité du gestionnaire de courrier qui vous permet de créer et de gérer des listes d'adresses e-mail et de domaines que vous pouvez utiliser dans les politiques de trafic et les ensembles de règles pour traiter le courrier entrant selon que le destinataire ou l'expéditeur d'un message appartient ou non à une liste spécifique. Les listes d'adresses permettent

un contrôle plus précis des flux de courrier électronique et contribuent à simplifier la gestion des scénarios complexes de routage des e-mails.

Que sont les listes d'adresses ?

Les listes d'adresses sont des conteneurs d'adresses e-mail et de domaines que vous pouvez utiliser pour filtrer et traiter les e-mails. Ils constituent un moyen pratique de regrouper les adresses associées et d'appliquer collectivement les règles de routage et les politiques de trafic.

Les principaux cas d'utilisation des listes d'adresses sont les suivants :

- Listes de refus pour bloquer des expéditeurs ou des domaines de spam connus
- Autoriser les listes pour garantir la livraison par des expéditeurs fiables
- Validation des destinataires pour rejeter de manière anticipée les e-mails envoyés à des destinataires inexistantes
- Routage basé sur les rôles pour appliquer différentes règles en fonction des rôles des destinataires
- Politiques basées sur les groupes pour appliquer les politiques à des groupes d'utilisateurs spécifiques

Comment fonctionnent les listes d'adresses

Les listes d'adresses de SES rationalisent la gestion des e-mails en vous permettant de créer et de gérer des ensembles d'adresses e-mail et de domaines. Une fois créées, ces listes sont intégrées à vos flux de travail de messagerie par le biais de politiques et de règles de trafic.

Lorsque SES traite un e-mail, il vérifie la liste d'adresses correspondante pour déterminer si l'expéditeur ou le destinataire est membre. Sur la base de cette adhésion et de vos politiques et règles configurées, SES prend ensuite les mesures appropriées, telles que le routage, le filtrage ou le rejet de l'e-mail. Ce processus permet un contrôle efficace et granulaire de votre trafic de courrier électronique.

Configuration de listes d'adresses

Rubriques

- [Création et remplissage d'une liste d'adresses](#)
- [Gestion des listes d'adresses](#)

Création et remplissage d'une liste d'adresses

La création d'une liste d'adresses dans la console consiste notamment à la renseigner avec une ou plusieurs adresses. À l'aide du gestionnaire de courrier APIs, vous pouvez créer des listes d'adresses vides et les remplir ultérieurement. Cette section vous montrera comment procéder à l'une ou l'autre à l'aide de procédures de console et AWS CLI d'exemples.

Pour créer et remplir une liste d'adresses :

1. Ouvrez la console SES à l'adresse <https://console.aws.amazon.com/ses/>.
2. Dans le volet de navigation, sous Mail Manager, sélectionnez Listes d'adresses.
3. Choisissez Créer une liste d'adresses et entrez un nom dans le champ Nom de la liste d'adresses.
4. Sélectionnez la saisie manuelle ou le téléchargement groupé et suivez les étapes correspondantes :
5. Pour la saisie manuelle : entrez une ou plusieurs adresses e-mail ou domaines dans la console.

Si vous utilisez le caractère générique astérisque (*), les formats suivants s'appliquent :

1. Un seul * est autorisé dans l'adresse :
 - Ce * doit être avant ou après @ lorsque l'entrée est une adresse e-mail.
 - Lorsqu'il * se trouve dans la partie locale, la partie locale peut comporter de zéro à 19 caractères, à l'exception du*.
 - Lorsqu'il * se trouve dans le domaine, le niveau du sous-domaine peut être compris entre 2 et 9, à l'exception du*.
2. Exemples de formats génériques valides :
 - *.domain1.com vers *.domain8.domain7... domain1.com
 - * @domain .com au 1234567890123456789* @domain .com
 - local@*.domain1.com vers local@*.domain8.domain7... domain1.com

Les caractères génériques peuvent être utilisés pour faire correspondre les adresses e-mail indépendamment des extensions de sous-adresses (plus l'adressage). Par exemple, l'ajout `user*@example.com` à une liste d'adresses correspondra à toute adresse dont la partie locale commence par `user` `user@example.com`, y compris `user+tag@example.com` `username@example.com`, etc.

6. Pour le téléchargement groupé : sélectionnez Choisir un fichier et choisissez un fichier CSV ou JSON sur votre ordinateur contenant les adresses à télécharger.

Utilisez le format indiqué dans l'exemple pour chaque type de fichier :

1. Exemple de fichier CSV (Notez que l'en-tête, `address`, est obligatoire.) :

```
address
user1@domain.com
user2@*.domain.com
*@domain.com
```

2. Exemple de fichier JSON :

```
{
  "items": [
    {
      "address": "user1@domain.com"
    },
    {
      "address": "user2@*.domain.com"
    },
    {
      "address": "@domain.com"
    }
  ]
}
```

7. Une fois que vous avez fini d'ajouter des adresses ou que vous avez sélectionné un fichier groupé, choisissez Créer une liste d'adresses.

En utilisant AWS CLI :

Création de la liste d'adresses

```
aws mailmanager create-address-list --address-list-name "MyDenyList"
```

Renseignez la liste d'adresses :

- Téléchargement unique

```
aws mailmanager register-member-to-address-list \
```

```
--address-list-id al-123456789abc \  
--address "user@example.com"
```

- Téléchargement groupé

Pour les téléchargements groupés, vous devez d'abord créer une tâche d'importation en spécifiant un format CSV ou JSON :

```
aws mailmanager create-address-list-import-job \  
--address-list-id "al-123456789abc" \  
--name "MyImportJob" \  
--import-data-format ImportDataType=CSV
```

Cela renvoie un identifiant de tâche et une URL pré-signée. Utilisez cette URL pré-signée pour télécharger votre fichier CSV ou JSON dans un compartiment S3, comme indiqué dans l'exemple suivant à l'aide de la commande curl :

```
curl -X PUT -T "/path/to/file" "pre-signed URL"
```

Après le téléchargement, lancez la tâche d'importation à l'aide de l'ID de tâche renvoyé dans la commande précédente :

```
aws mailmanager start-address-list-import-job --job-id "job-123456789"
```

Gestion des listes d'adresses

Vous pouvez mettre à jour, consulter et supprimer des listes d'adresses selon vos besoins.

Rubriques

- [Mettre à jour une liste d'adresses](#)
- [Afficher les détails de la liste d'adresses](#)
- [Supprimer une liste d'adresses](#)

Mettre à jour une liste d'adresses

Vous pouvez mettre à jour une liste d'adresses en ajoutant ou en supprimant des adresses, et éventuellement en ajoutant ou en supprimant des balises.

Pour mettre à jour une liste d'adresses :

1. Sur la page Listes d'adresses, sélectionnez le nom de la liste d'adresses que vous souhaitez modifier.
2. Pour ajouter des adresses, choisissez Ajouter une adresse e-mail et procédez à la saisie manuelle ou à la méthode de téléchargement groupé, comme expliqué dans [Création et remplissage d'une liste d'adresses](#).
3. Pour supprimer des adresses, cochez la case à côté de chaque adresse que vous souhaitez supprimer, puis cliquez sur Supprimer l'adresse e-mail et confirmez la suppression.
4. (Facultatif) Ajoutez ou supprimez des balises à votre liste d'adresses en choisissant Gérer les balises.

En utilisant AWS CLI :

Addition

```
aws mailmanager register-member-to-address-list \  
    --address-list-id al-123456789abc \  
    --address "user@example.com"
```

Supprimez

```
aws mailmanager deregister-member-from-address-list \  
    --address-list-id al-123456789abc \  
    --address "user@example.com"
```

Afficher les détails de la liste d'adresses

Pour consulter les détails de la liste d'adresses :

- Sur la page Listes d'adresses, sélectionnez le nom d'une liste d'adresses pour en afficher les détails.

En utilisant AWS CLI :

```
aws mailmanager list-members-of-address-list --address-list-id al-123456789abc
```

Supprimer une liste d'adresses

Pour supprimer une liste d'adresses :

1. Sur la page Listes d'adresses, sélectionnez le bouton radio à côté de la liste d'adresses que vous souhaitez supprimer, puis cliquez sur Supprimer.
2. Confirmez la suppression de la liste en tapant « confirmer » puis « Supprimer ».

En utilisant AWS CLI :

```
aws mailmanager delete-address-list --address-list-id a1-123456789abc
```

Utilisation de listes d'adresses dans les politiques de trafic et les ensembles de règles

Les listes d'adresses peuvent être utilisées dans les déclarations de politique de trafic et les conditions de règles pour traiter les e-mails en fonction de l'appartenance aux listes, ce qui permet de contrôler le flux d'e-mails. Les sections suivantes fournissent un exemple de listes d'adresses utilisées dans le cadre d'une politique de trafic et d'un ensemble de règles.

Rubriques

- [Utilisation d'une liste d'adresses dans une déclaration de politique de trafic](#)
- [Utilisation d'une liste d'adresses dans une règle](#)

Utilisation d'une liste d'adresses dans une déclaration de politique de trafic

Les listes d'adresses peuvent être sélectionnées lorsque vous créez les conditions d'une déclaration de politique de trafic pour autoriser ou refuser l'entrée d'e-mails sur votre point de terminaison d'entrée.

La procédure de console suivante et son AWS CLI équivalent montrent un exemple de création d'une déclaration de politique autorisant l'entrée de messages dans votre point de terminaison d'entrée si le destinataire figure dans la liste d'adresses spécifiée.

Pour utiliser une liste d'adresses dans une déclaration de politique de trafic :

1. Créez une nouvelle politique de trafic ou modifiez une politique existante comme expliqué dans [Création de politiques de trafic et de déclarations de politique \(console\)](#)

2. Dans le conteneur de la déclaration de politique, choisissez Autoriser pour que l'action soit entreprise lorsque les conditions de la déclaration sont remplies.
3. Construisez la condition de la déclaration comme suit :
 - Sélectionnez l'adresse du destinataire dans le champ Protocole.
 - Sélectionnez Se trouve dans la liste d'adresses pour le champ Opérateur.
 - Sélectionnez le nom de votre liste d'adresses dans le champ Valeur.
4. Bien qu'il ne s'agisse que d'un exemple, vous pouvez ajouter d'autres conditions de politique qui peuvent être basées sur divers opérateurs avec n'importe laquelle de vos listes d'adresses.

En utilisant AWS CLI :

```
aws mailmanager create-traffic-policy \  
  --default-action ALLOW \  
  --traffic-policy-name "testpolicy" \  
  --policy-statements '[{  
    "Action": "ALLOW",  
    "Conditions": [{  
      "BooleanExpression": {  
        "Evaluate": {  
          "IsInAddressList": {  
            "Attribute": "RECIPIENT",  
            "AddressLists": [  
              "arn:aws:ses:eu-west-3:123456789012:mailmanager-address-  
list/al-123456789abc"  
            ]  
          }  
        },  
        "Operator": "IS_TRUE"  
      }  
    ]  
  }]  
}]'
```

Utilisation d'une liste d'adresses dans une règle

Les listes d'adresses peuvent être sélectionnées lorsque vous créez la condition d'une règle utilisée dans l'un de vos ensembles de règles pour déclencher l'action de la règle.

La procédure de console suivante et son AWS CLI équivalent montrent un exemple de création d'une règle qui invoque l'action de suppression si le destinataire figure dans la liste d'adresses spécifiée.

Pour utiliser une liste d'adresses dans une condition de règle :

1. Créez une nouvelle règle ou modifiez une règle existante comme expliqué dans [Création d'ensembles de règles et de règles \(console\)](#)
2. Dans le conteneur Conditions de règle, créez la condition de la règle comme suit.
 - Sélectionnez l'adresse du destinataire dans le champ Sélectionner la propriété.
 - Sélectionnez Se trouve dans la liste d'adresses pour le champ Sélectionner un opérateur.
 - Sélectionnez le nom de votre liste d'adresses dans le champ Valeur.
3. Dans le conteneur Actions, choisissez Ajouter une nouvelle action et sélectionnez Supprimer l'action.
4. Bien qu'il ne s'agisse que d'un exemple, vous pouvez ajouter d'autres conditions de règle qui peuvent être basées sur différents opérateurs avec n'importe laquelle de vos listes d'adresses pour une variété d'actions à entreprendre.

En utilisant AWS CLI :

```
aws mailmanager create-rule-set \  
  --rule-set-name "testruleset2" \  
  --rules '[{  
    "Name": "addresslist",  
    "Conditions": [{  
      "BooleanExpression": {  
        "Evaluate": {  
          "IsInAddressList": {  
            "Attribute": "RECIPIENT",  
            "AddressLists": [  
              "arn:aws:ses:us-east-1:123456789012:mailmanager-address-  
list/al-123456789abc"  
            ]  
          }  
        },  
        "Operator": "IS_TRUE"  
      }  
    ],  
    "Actions": [{  
      "Drop": {}  
    }]  
  }]
```

Bonnes pratiques et considérations

- Faites attention à la taille des listes : les listes très volumineuses peuvent avoir un impact sur les performances.
- Les listes d'adresses sont spécifiques au compte et ne peuvent être utilisées que dans le même AWS compte.
- Les listes d'adresses imbriquées ne sont actuellement pas prises en charge.
- Un maximum de 100 listes d'adresses par région est pris en charge.
- Un maximum de 100 000 adresses par liste d'adresses est pris en charge.

Archivage des e-mails

L'archivage des e-mails vous permet d'archiver les types d'e-mails que vous spécifiez pour votre point de terminaison d'entrée, ou les e-mails que vous envoyez via un ensemble de configuration, 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.

Une archive peut contenir une combinaison d'e-mails envoyés et reçus :

- Archivage des e-mails envoyés : lorsque vous envoyez des e-mails (sortants) via un ensemble de configuration avec l'option d'archivage activée, tous les e-mails envoyés à l'aide de ce jeu de configuration sont archivés dans l'archive d'e-mails que vous désignez.
- Archivage des e-mails reçus : lorsque votre point de terminaison d'entrée reçoit des e-mails (entrants), 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 spécifier dans une action de règle ou un ensemble de configuration. 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 tables interactives, 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. Maintenant que vous avez créé une archive, vous pouvez l'utiliser dans un [ensemble de règles](#) pour archiver les e-mails reçus (entrants) ou la désigner dans un [ensemble de configuration](#) pour archiver les e-mails envoyés (sortants).
6. 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.

7. Pour supprimer une archive, sélectionnez le bouton radio correspondant puis 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.

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 vous concentrer sur la prévention des 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 l'envoi d'e-mails dans 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 :

Exemple de politique de trafic utilisant un module complémentaire

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 :

▼ Policy statement Info Remove

Allow or deny properties
Choose the action to be taken when the filter conditions are met.

Deny

Protocol	Operator	Value
Is listed (Spamhaus Domain Block List)	Equals	FALSE

Add new condition

You can add 9 more filter conditions

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, consultez [the section called “Création de politiques de trafic et de déclarations de politique \(console\)”](#).

Exemple de condition de règle utilisant un module complémentaire

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 :

Rule conditions Info

Select property: Is passed (Trend Micro Virus Scanning) ▼

Select operator: Equals ▼

Value: True ▼

Remove

Add new condition

☐ EXCEPT in the case of:

Pour plus de détails sur la façon de créer des ensembles de règles et de créer des conditions de règles avec Email Add Ons, consultez [the 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, consultez [the 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.

JSON

```
{
  "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

Il est nécessaire d'utiliser une clé gérée par le client (CMK) pour votre secret. La déclaration suivante est requise dans le cadre de votre politique de clé KMS pour permettre à SES d'utiliser votre clé pour 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/*"
        }
    }
}

```

Politique de clé gérée par le client (CMK) de KMS pour le magasin de confiance de MTL

Si vous utilisez une clé gérée par le client (CMK) pour chiffrer votre magasin de confiance mTLS, la déclaration suivante est requise dans votre politique de clé KMS pour permettre à SES d'utiliser votre clé.

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "ses.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "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, consultez [the 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.

JSON

```
{
  "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 déclaration suivante est requise dans le cadre de votre politique de clé KMS pour permettre à SES d'utiliser votre clé pour votre secret.

JSON

```
{
  "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

Archivage et exportation

L'appelant d'identité IAM `StartArchiveExport` doit avoir accès au compartiment S3 de destination configuré selon la politique IAM suivante :

JSON

```

{
  "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/*"
  }
]
}

```

Voici la politique du compartiment S3 pour le compartiment de destination :

JSON

```

{
  "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

L'identité IAM appelle CreateArchive et UpdateArchive doit avoir accès à l'ARN de la clé KMS conformément à la politique suivante :

JSON

```

{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:DescribeKey",
      "kms:Decrypt",
      "kms:GenerateDataKey"
    ],
    "Resource": "arn:aws:kms:us-east-1:111122223333:key/MyKmsKeyArnID"
  }
}

```

Les déclarations suivantes sont obligatoires dans le cadre de votre politique relative aux clés KMS :

JSON

```
{
  "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 Gestion des identités et des accès AWS (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 chaque action de règle spécifique.

JSON

```
{
  "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/*"
        }
      }
    }
  ]
}
```

Politiques d'action relatives aux règles

- [Politique d'autorisation pour l'action de la règle Write to S3](#)
- [Politique d'autorisation pour l'action relative à la règle de livraison dans une boîte aux lettres](#)
- [Politique d'autorisation pour l'action des règles d'envoi vers Internet](#)
- [Politique d'autorisation pour l'action relative à la règle Deliver to Q Business](#)
- [Politique d'autorisation pour l'action des règles de publication sur les réseaux sociaux](#)
- [Politique d'autorisation pour l'action de la règle Bounce](#)
- [Politique d'autorisation pour l'action de la règle de la fonction Invoke Lambda](#)

Politique d'autorisation pour l'action de la règle Write to S3

La politique suivante est requise pour que votre rôle IAM utilise l'action de règle Write to S3 qui envoie le courrier électronique reçu à un compartiment S3.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPutObject",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::MyDestinationBucketName/*"
      ]
    },
    {
      "Sid": "AllowListBucket",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::MyDestinationBucketName"
      ]
    }
  ]
}
```

```
}
```

Si vous utilisez une clé gérée par le AWS KMS client pour un compartiment S3 sur lequel le chiffrement côté serveur est activé, vous devez ajouter l'action de politique de rôle IAM, "kms:GenerateDataKey*" Dans l'exemple précédent, l'ajout de cette action à votre politique de rôle se présenterait comme suit :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowKMSKeyAccess",
      "Effect": "Allow",
      "Action": "kms:GenerateDataKey*",
      "Resource": "arn:aws:kms:us-east-1:888888888888:key/*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "kms:ResourceAliases": [
            "alias/MyKeyAlias"
          ]
        }
      }
    }
  ]
}
```

Pour plus d'informations sur l'association de politiques aux AWS KMS clés, consultez la section [Utilisation des politiques clés AWS KMS dans](#) le manuel du AWS Key Management Service développeur.

Politique d'autorisation pour l'action relative à la règle de livraison dans une boîte aux lettres

La politique suivante est requise pour que votre rôle IAM utilise l'action de règle Deliver to mailbox qui envoie l'e-mail reçu à un WorkMail compte Amazon.

JSON

```
{
  "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 que votre rôle IAM utilise l'action de règle Envoyer vers Internet qui envoie l'e-mail reçu à un domaine externe.

 Note

Si votre identité SES utilise un ensemble de configuration par défaut, vous devez également ajouter la ressource d'ensemble de configuration, comme indiqué dans l'exemple suivant.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["ses:SendEmail", "ses:SendRawEmail"],
      "Resource": [
        "arn:aws:ses:us-east-1:888888888888:identity/example.com",
        "arn:aws:ses:us-east-1:888888888888:configuration-set/my-configuration-set"
      ]
    }
  ]
}
```

```
]
}
```

Politique d'autorisation pour l'action relative à la règle Deliver to Q Business

Les politiques suivantes sont requises pour utiliser l'action de règle Deliver to Q Business, qui envoie le courrier électronique reçu vers un index Amazon Q Business.

Politique IAM requise pour votre rôle :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccessToQBusiness",
      "Effect": "Allow",
      "Action": [
        "qbusiness:BatchPutDocument"
      ],
      "Resource": [
        "arn:aws:qbusiness:us-  
east-1:888888888888:application/ApplicationID/index/IndexID"
      ]
    }
  ]
}
```

Déclaration requise dans le cadre de votre politique relative aux clés KMS :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccessToKMSKeyForQbusiness",
      "Effect": "Allow",
```

```

    "Action": [
        "kms:GenerateDataKey*",
        "kms:Encrypt",
        "kms:DescribeKey"
    ],
    "Resource": [
        "arn:aws:kms:us-east-1:888888888888:key/*"
    ],
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "qbusiness.us-east-1.amazonaws.com",
            "kms:CallerAccount": "888888888888"
        },
        "ForAnyValue:StringEquals": {
            "kms:ResourceAliases": [
                "alias/MyKeyAlias"
            ]
        }
    }
}

```

Pour plus d'informations sur l'association de politiques aux AWS KMS clés, consultez la section [Utilisation des politiques clés AWS KMS dans](#) le manuel du AWS Key Management Service développeur.

Politique d'autorisation pour l'action des règles de publication sur les réseaux sociaux

Les politiques suivantes sont requises pour utiliser l'action de règle Publier sur SNS, qui envoie l'e-mail reçu à une rubrique Amazon SNS.

Politique IAM requise pour votre rôle :

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAccessToSNSTopic",

```

```

        "Effect": "Allow",
        "Action": [
            "sns:Publish"
        ],
        "Resource": [
            "arn:aws:sns:us-east-1:888888888888:MySnsTopic"
        ]
    }
]
}

```

Déclaration requise dans le cadre de votre politique relative aux clés KMS :

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAccessToKMSKeyForSNS",
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Encrypt",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:888888888888:key/*"
            ],
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "qbusiness.us-east-1.amazonaws.com",
                    "kms:CallerAccount": "888888888888"
                },
                "ForAnyValue:StringEquals": {
                    "kms:ResourceAliases": [
                        "alias/MyKeyAlias"
                    ]
                }
            }
        }
    ]
}

```

```
}
```

Pour plus d'informations sur l'association de politiques aux AWS KMS clés, consultez la section [Utilisation des politiques clés AWS KMS dans](#) le manuel du AWS Key Management Service développeur.

Politique d'autorisation pour l'action de la règle Bounce

La politique suivante est requise pour que votre rôle IAM utilise l'action de règle Bounce qui fait rebondir l'e-mail en renvoyant une réponse de rebond à l'expéditeur.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSendBounce",
      "Effect": "Allow",
      "Action": [
        "ses:SendBounce"
      ],
      "Resource": [
        "arn:aws:ses:us-east-1:123456789012:identity/*"
      ],
      "Condition": {
        "StringEquals": {
          "ses:FromAddress": "sender@example.com"
        }
      }
    }
  ]
}
```

Politique d'autorisation pour l'action de la règle de la fonction Invoke Lambda

La politique suivante est requise pour que votre rôle IAM utilise l'action de règle de la fonction Invoke Lambda qui appelle AWS Lambda une fonction pour traiter le courrier électronique.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
{
  "Sid": "AllowInvokeLambdaFunction",
  "Effect": "Allow",
  "Action": [
    "lambda:InvokeFunction"
  ],
  "Resource": [
    "arn:aws:lambda:us-east-1:123456789012:function:MyFunction"
  ]
}
```

Journalisation du gestionnaire de courrier

La journalisation du gestionnaire de courrier fournit une visibilité détaillée des opérations de votre gestionnaire de courrier. La fonctionnalité de journalisation suit le flux des messages depuis leur réception initiale aux points de terminaison d'entrée jusqu'au traitement des messages en fonction des ensembles de règles et des règles que vous avez configurés.

Mail Manager propose la journalisation des ressources suivantes :

- Points de terminaison d'entrée
- Ensemble de règles

Mail Manager fournit les journaux à l'aide du service Amazon CloudWatch Logs et les journaux peuvent être envoyés vers l'une des destinations suivantes : CloudWatch Logs, Amazon S3 ou Amazon Data Firehose.

Configuration de la livraison du journal Mail Manager

La livraison d'un journal de travail comprend trois éléments :

- **DeliverySource**— Un objet logique qui représente la ressource qui envoie les journaux, qu'il s'agisse d'un point de terminaison d'entrée ou d'un ensemble de règles.
- **DeliveryDestination**— Un objet logique qui représente la destination de livraison réelle (CloudWatch Logs, S3 ou Firehose).
- **Livraison** : connecte une source de livraison à une destination de livraison.

Cette section explique comment créer ces objets ainsi que les autorisations nécessaires pour utiliser la journalisation de Mail Manager.

Conditions préalables

Avant de configurer la journalisation de Mail Manager, assurez-vous que :

1. Vous avez créé un point de [terminaison Ingress](#) ou un [ensemble de règles](#).
2. Vous disposez des autorisations nécessaires en matière de CloudWatch journaux et de SES Mail Manager pour vendre les journaux des ressources de votre gestionnaire de courrier à leurs destinations de livraison.

Autorisations requises

Vous devez configurer les autorisations relatives aux journaux vendus, comme expliqué dans la section [Journalisation nécessitant des autorisations supplémentaires \[V2\]](#) du guide de l'utilisateur d'Amazon CloudWatch Logs, et appliquer les autorisations correspondant à votre destination de livraison :

- [Logs envoyés à CloudWatch Logs](#)
- [Journaux envoyés à Amazon S3](#)
- [Logs envoyés à Firehose](#)

En outre, Mail Manager nécessite les autorisations utilisateur suivantes pour configurer la remise des journaux :

- `ses:AllowVendedLogDeliveryForResource`— Nécessaire pour autoriser Mail Manager à vendre les journaux en votre nom à CloudWatch Logs pour vos ressources spécifiques, comme indiqué dans l'exemple :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSesMailManagerLogDelivery",
      "Effect": "Allow",
```

```

        "Action": [
            "ses:AllowVendedLogDeliveryForResource"
        ],
        "Resource": [
            "arn:aws:ses:us-east-1:111122223333:mailmanager-ingress-point/inp-
xxxxx",
            "arn:aws:ses:us-east-1:111122223333:mailmanager-rule-set/rs-xxxx"
        ]
    }
}

```

Activation de la connexion dans la console SES

Pour activer la journalisation des ressources de Mail Manager à l'aide de la console :

1. Ouvrez la console SES à l'adresse <https://console.aws.amazon.com/ses/>.
2. Dans le volet de navigation, sous Mail Manager, choisissez soit les points de terminaison d'entrée, soit les ensembles de règles, puis sélectionnez la ressource spécifique que vous souhaitez activer pour la journalisation.
3. Sur la page de détails de la ressource, développez Add log delivery et choisissez la livraison vers CloudWatch Logs, S3 ou Firehose.
4. Dans la boîte de dialogue Ajouter la livraison à la destination que vous avez choisie, suivez les instructions pour configurer les options de livraison du journal spécifiques au type de destination.
5. (Facultatif) Développez les paramètres supplémentaires pour personnaliser les champs de l'enregistrement, le format de sortie, le délimiteur de champs et d'autres paramètres spécifiques au type de destination.

Activer la journalisation à l'aide de l'API CloudWatch Logs

Pour activer la journalisation des ressources Mail Manager à l'aide de l'API CloudWatch Logs, vous devez :

1. Créez un DeliverySource avec [PutDeliverySource](#).
2. Créez un DeliveryDestination avec [PutDeliveryDestination](#).
3. Créez une livraison en associant exactement une source de livraison et une destination de livraison en utilisant [CreateDelivery](#).

Vous pouvez consulter des exemples de règles de rôle et d'autorisations IAM avec toutes les autorisations requises pour votre destination de journalisation spécifique dans la section [Journalisation nécessitant des autorisations supplémentaires \[V2\]](#) du guide de l'utilisateur Amazon CloudWatch Logs, et suivre les exemples de règles de rôle et d'autorisations IAM pour votre destination de journalisation, notamment en autorisant les mises à jour de votre ressource de destination de journalisation spécifique, telle que CloudWatch Logs, S3 ou Firehose.

Note

Lors de la création d'un DeliverySource, il [resourceArn](#) peut s'agir d'un ARN de point de terminaison d'entrée ou d'un ARN d'ensemble de règles. En fonction du DeliverySource, cela [logType](#) peut être le suivant :

- ARN du point de terminaison d'entrée — ou APPLICATION_LOGS
TRAFFIC_POLICY_DEBUG_LOGS
- Ensemble de règles ARN — APPLICATION_LOGS

Interprétation des journaux

Les journaux peuvent être utilisés pour obtenir des informations supplémentaires sur le flux de vos messages reçus au fur et à mesure qu'ils sont traités par Mail Manager.

Les exemples suivants détaillent les différents champs des journaux pour chaque ressource et chaque type de journal :

Exemples de journaux

- [Journaux des terminaux entrants — APPLICATION_LOGS](#)
- [Journaux des terminaux entrants — TRAFFIC_POLICY_DEBUG_LOGS](#)
- [Journaux des ensembles de règles — APPLICATION_LOGS](#)

Journaux des terminaux entrants — **APPLICATION_LOGS**

Les journaux sont générés par message.

```
{  
  "resource_arn": "arn:aws:ses:us-east-1:1234567890:mailmanager-ingress-point/inp-  
xxxxx",
```

```

"event_timestamp": 1728562395042,
"ingress_point_type": "OPEN" | "AUTH" | "MTLS",
"ingress_point_name": "MyIngressPoint",
"message_id": "000011lckiljmushh817gr586f963a5inhkvn81",
"message_size_bytes": 100000,
"rule_set_id": "rs-xxxx",
"sender_ip_address": "1.2.3.4",
"smtp_mail_from": "someone@domain.com",
"smtp_helo": "domain.com",
"tls_protocol": "TLSv1.2",
"tls_cipher_suite": "TLS_AES_256_GCM_SHA384",
"recipients": ["me@mydomain.com", "you@mydomain.com", "they@mydomain.com"],
"ingress_point_metadata": {
    // Only applies to AUTH Ingress endpoint
    "password_version": "",
    "secrets_manager_arn": "",
    // Only applies to MTLS Ingress endpoint
    "client_certificate_details": {
        "common_names": ["mail.example.com"],
        "serial_number": "0A:DE:EB:89:42:FB:1C:67",
        "subject_alternative_names": ["mail.example.com", "smtp.example.com"],
        "issuer": "CN=Example CA,O=Example Corp,C=US",
        "not_before": "2025-01-15T00:00:00Z",
        "not_after": "2026-01-15T23:59:59Z"
    },
    "trust_store_monitoring": {
        "ca_invalid_or_near_expiry": [
            {
                "subject": "CN=Example CA,O=Example Corp,C=US",
                "not_before": "2023-06-01T00:00:00Z",
                "not_after": "2025-05-15T23:59:59Z"
            },
            ...
        ],
        "crl_invalid_or_near_expiry": [
            {
                "issuer": "CN=Example CA,O=Example Corp,C=US",
                "this_update": "2025-03-01T00:00:00Z",
                "next_update": "2025-04-01T00:00:00Z"
            },
            ...
        ]
    }
}

```

```
}
```

Note

Les journaux sont créés uniquement pour les messages acceptés par le point de terminaison d'entrée. Un point de terminaison d'entrée qui rejette tous les messages entrants ne publiera aucun journal d'application.

Note

Les `trust_store_monitoring` listes (`ca_invalid_or_near_expiry` et `crl_invalid_or_near_expiry`) renvoient chacune un maximum de 10 entrées. « Proche d'expiration » signifie que le certificat ou la CRL expire dans les 90 jours.

Exemples de requêtes CloudWatch Logs Insights

Messages de requête provenant de `sender@domain.com` :

```
fields @timestamp, @message, @logStream, @log
| filter smtp_mail_from like /sender@domain.com/
| sort @timestamp desc
| limit 10000
```

Messages de requête d'une taille supérieure à 5 000 octets :

```
fields @timestamp, @message, @logStream, @log
| filter message_size_bytes > 5000
| sort @timestamp desc
| limit 10000
```

Journaux des terminaux entrants — **TRAFFIC_POLICY_DEBUG_LOGS**

Les journaux sont générés par destinataire.

```
{
  "resource_arn": "arn:aws:ses:us-east-1:1234567890:mailmanager-ingress-point/inp-xxxxx",
```

```

"event_timestamp": 1728562395042,
"ingress_point_type": "OPEN" | "AUTH",
"ingress_point_id": "inp-xxxx",
"ingress_point_session_id": "xxxx",
"traffic_policy_id": "tp-xxxx",
"traffic_policy_evaluation": [
    // Array of policy evaluations
    {
        "action": "ALLOW" | "DENY",
        "conditions": [
            // Array of conditions
            {
                "expression": {
                    "attribute": "RECIPIENT",
                    "operator": "CONTAINS",
                    "value": ["@domain.com", "@mydomain.com"]
                },
                "expressionResult": true | false
            },
            "policyStatementMatched": true | false
        ],
        "policyStatementMatched": true | false
    },
    // If no policy statement match then default action will be applied
    {
        "action": "ALLOW" | "DENY",
        "policyStatementMatched": true,
        "type": "DefaultAction",
        "scope": "Recipient"
    },
    // Only present if the email was too large according to the traffic policy
    {
        "action": "DENY",
        "allowedMessageSize": 41943040,
        "receivedMessageSize": 42495384,
        "scope": "Data"
    }
],
"traffic_policy_verdict": "REJECT" | "ACCEPT",
"sender_ip_address": "1.2.3.4",
"smtp_mail_from": "someone@domain.com",
"smtp_helo": "domain.com",
"tls_protocol": "TLSv1.2",
"recipient": "me@mydomain.com",
"tls_cipher_suite": "TLS_AES_256_GCM_SHA384"

```

```
}
```

Note

- Des journaux sont créés pour tous les messages évalués par la politique de trafic au niveau du point de terminaison d'entrée, qu'ils soient acceptés ou rejetés.
- Toutes les évaluations de la politique de trafic des destinataires relatives au même message (dans le cadre d'une même conversation SMTP) ont un point commun `ingress_point_session_id`. Cet identifiant sert d'identifiant de corrélation puisqu'il `message_id` n'est disponible qu'après acceptation du message.
- Le `traffic_policy_evaluation` contenu varie en fonction de votre configuration et peut être annulé plus tôt qu'un verdict aura été rendu.

Exemples de requêtes CloudWatch Logs Insights

Messages de requête provenant de `sender@domain.com` :

```
fields @timestamp, @message, @logStream, @log
| filter smtp_mail_from like /sender@domain.com/
| sort @timestamp desc
| limit 10000
```

Interrogez les messages appartenant à un utilisateur spécifique `ingress_point_session_id` :

```
fields @timestamp, @message, @logStream, @log
| filter ingress_point_session_id = 'xxx'
| sort @timestamp desc
| limit 10000
```

Messages de requête qui ont été rejetés :

```
fields @timestamp, @message, @logStream, @log
| filter traffic_policy_verdict = 'REJECT'
| sort @timestamp desc
| limit 10000
```

Journaux des ensembles de règles — APPLICATION_LOGS

Les journaux sont générés par message et par action. Cela signifie qu'un enregistrement de journal est généré chaque fois qu'un message est traité par une action dans une règle du jeu de règles :

```
{
  "resource_arn": "arn:aws:ses:us-east-1:1234567890:mailmanager-rule-set/rs-xxxx",
  "event_timestamp": 1732298258254,
  "message_id": "00001lckiljmushh817gr586f963a5inhkvn81",
  "rule_set_name": "MyRuleSet",
  "rule_name": "MyRule",
  "rule_index": 1,
  "recipients_matched": ["recipient1@domain.com", "recipient2@domain.com"],
  "action_metadata": {
    "action_name": "WRITE_TO_S3" | "DROP" | "RELAY" | "DELIVER_TO_MAILBOX" | etc.,
    "action_index": 2,
    "action_status": "SUCCESS" | "FAILURE" | "IN_PROGRESS",
    "action_failure": "Access denied"
  }
}
```

- **recipients_matched**— Les destinataires auxquels les conditions de la règle pour laquelle l'action est exécutée correspondent.
- **rule_index**— L'ordre de la règle au sein de l'ensemble de règles.
- **action_index**— L'ordre de l'action dans le cadre de la règle.
- **action_status**— Indique le résultat de l'exécution de l'action sur le message donné.
- **action_failure**— Indique les détails de l'échec de l'action (ne s'applique qu'en cas d'échec d'une action). Par exemple, si le rôle fourni ne dispose pas des autorisations suffisantes pour effectuer l'action.

En outre, si les conditions de la règle ne correspondent pas pour un message, c'est-à-dire que le message n'est pas traité par la règle, un seul journal est publié pour indiquer que le message a été traité par l'ensemble de règles, mais qu'aucune action n'a été effectuée sur celui-ci :

```
{
  "resource_arn": "arn:aws:ses:us-east-1:1234567890:mailmanager-rule-set/rs-xxxx",
  "event_timestamp": 1732298258254,
  "message_id": "00001lckiljmushh817gr586f963a5inhkvn81",
  "rule_set_name": "MyRuleSet",
```



```
"rule_name": "MyRule",  
"rule_index": 1,  
"recipients_matched": [],  
}
```

Exemples de requêtes CloudWatch Logs Insights

Requête pour un identifiant de message spécifique (indique le flux des messages dans l'ensemble de règles) :

```
fields @timestamp, @message, @logStream, @log  
| filter message_id = 'message-id-123'  
| sort @timestamp desc  
| limit 10000
```

Requête concernant les actions WRITE_TO_S3 ayant échoué :

```
fields @timestamp, @message, @logStream, @log  
| filter action_metadata.action_name = 'WRITE_TO_S3'  
    and action_metadata.action_status = 'FAILURE'  
| sort @timestamp desc  
| limit 10000
```

Requête pour les messages qui n'ont pas été traités par la deuxième règle d'un ensemble de règles (le message ne répondait pas aux conditions de la règle) :

```
fields @timestamp, @message, @logStream, @log  
| filter recipients_matched = '[]'  
    and rule_index = 2  
| sort @timestamp desc  
| limit 10000
```

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 préserver votre réputation d'expéditeur, SES propose une suppression au niveau du compte, au niveau du locataire et au niveau de l'ensemble de configuration qui vous empêche d'envoyer à des destinataires non valides et de nuire à votre réputation d'expéditeur. Si vous utilisez le multitenant, les listes de suppression au niveau des locataires fournissent à chaque locataire sa propre liste de suppression isolée, empêchant ainsi toute contamination entre locataires. 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 décrit en détail dans les sections répertoriées dans les rubriques de ce chapitre ; toutefois, un aperçu des listes de suppression est présenté ici pour comprendre en quoi elles diffèrent, ainsi que l'un des principaux changements apportés à 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.

Vue d'ensemble des listes de suppression et du mécanisme de dérogation

La fonctionnalité de suppression de la liste de suppression globale n'est plus destinée aux clients et vous n'interagissez plus avec elle pour gérer la suppression. La liste de suppression globale fonctionne et est gérée en arrière-plan par SES. En tant que client, vous avez désormais à votre disposition une liste de suppression au niveau du compte et des options de suppression au niveau des ensembles de configuration qui vous offrent un contrôle plus personnalisé sur la manière 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.

- Liste de suppression globale : détenue et gérée par SES afin de protéger la réputation des adresses du pool d'adresses IP partagé de SES.
- Account-level liste de suppression, détenue et gérée par le client pour protéger la réputation de son compte, remplace la liste de suppression globale.

- Suppression au niveau de l'ensemble de configuration : mécanisme de dérogation destiné à fournir un contrôle conditionnel ou précis de la liste de suppression au niveau du compte grâce à l'utilisation des remplacements spécifiés dans un ensemble de configuration.

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'interagissiez plus directement avec la liste de suppression globale, celle-ci fonctionne toujours en arrière-plan et les principes généraux du fonctionnement de la liste de suppression globale peuvent également être appliqués pour expliquer les principes généraux du fonctionnement des autres types 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 leur propre liste de suppression et leur propre réputation. Ainsi, la liste de suppression au niveau du compte ne s'applique qu'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](#).

Suppression au niveau de l'ensemble de configuration, bien qu'il ne s'agisse pas d'une liste en soi, mais d'un mécanisme qui vous permet de configurer des personnalisations de suppression et de remplacer la liste de suppression au niveau de votre compte en utilisant des ensembles de configuration spécialement 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 fonctionnalité de demande de suppression d'adresses e-mail de la liste de suppression globale n'est plus destinée aux clients et vous n'interagissez plus avec elle pour gérer la suppression. Pour remplacer cette fonctionnalité, Amazon SES propose désormais une nouvelle méthode pour gérer votre suppression en mettant à disposition une liste de suppression au niveau du compte et des remplacements de suppression au niveau des ensembles de configuration qui vous offrent un contrôle plus personnalisé sur la manière dont vous gérez la suppression des e-mails pour votre propre compte. Pour plus d'informations, consultez [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 important de comprendre les liens entre les listes de suppression SES et leur hiérarchie, voir [Présentation des listes de suppression et du mécanisme de dérogation à la 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 leur propre liste de suppression et gérer leur réputation. Ainsi, votre liste de suppression au niveau du compte ne s'applique qu'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

Si vous utilisez le multitenant, vous pouvez également configurer des listes de suppression au niveau des locataires pour une isolation par locataire. Lorsque la suppression au niveau du locataire est activée pour un locataire, SES utilise la liste de suppression du locataire au lieu de la liste de suppression au niveau du compte. Pour de plus amples informations, veuillez consulter [Utilisation de listes de suppression au niveau des locataires dans Amazon 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 \(sortie du sandbox d'Amazon SES\)](#).

 Important

Les listes de suppression de comptes SES distinguent les majuscules et minuscules. Lorsqu'une adresse e-mail est ajoutée à la liste de suppression, User@ Example.com, elle est enregistrée exactement telle qu'elle a été reçue, en préservant le dossier d'origine. Bien que la fonctionnalité d'envoi d'e-mails traite les adresses présentant des cas différents comme identiques (par exemple, User@ Example.com est identique à user@example.com), les appels d'API pour la gestion des listes de suppression nécessitent une correspondance exacte entre les cas. Ainsi, lorsque vous utilisez des API liées à la gestion des listes de suppression, assurez-vous d'utiliser le cas exact de l'adresse e-mail telle qu'elle apparaît dans la liste de suppression.

Considérations relatives à Account-level la liste de suppression 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. Cependant, SES essaiera de livrer les adresses figurant dans la liste de suppression au niveau de votre compte avec le motif de suppression de la réclamation (car dans ce cas, elles ne correspondent pas).
- 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.
- SES ne prend pas en compte les messages que vous envoyez aux adresses figurant sur la liste de suppression au niveau de votre compte dans les Reputation.ComplaintRateMetrics Reputation.BounceRate ou dans l'espace de noms AWS/SES de votre compte. Ces messages sont comptabilisés dans les métriques Bounce ou Complaint dans l'espace de noms AWS/SSE.
- 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'[CreateImportJob](#) opération [PutSuppressedDestination](#) tant que votre compte n'est pas supprimé du 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.

Note

Les procédures décrites dans les sections suivantes supposent que vous avez déjà installé le 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](#).

Activation de la liste de suppression au niveau du compte Amazon SES

Vous pouvez utiliser l'[PutAccountSuppressionAttributes](#) opération dans l'API Amazon SES v2 pour activer et configurer votre liste de suppression au niveau du 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 du 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 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 Suppression list (Liste de suppression).
3. Dans le volet des Account-level paramètres, choisissez 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. Sélectionnez 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.

Pour configurer votre liste de suppression au niveau du compte pour un ensemble de configuration à l'aide du 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 configuration qui doit utiliser votre liste de suppression au niveau du 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 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. 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. Sélectionnez **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 en utilisant l'[PutSuppressedDestination](#) opération de 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.

Pour ajouter des adresses individuelles à la liste de suppression au niveau de votre compte à l'aide du 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 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 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 masse en téléchargeant d'abord votre liste de contacts dans un objet Amazon S3, puis en utilisant l'[CreateImportJob](#) opération 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.
- Vous ne pouvez pas exécuter plus de 20 tâches d'importation simultanées.
- 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 par *recipient2@example.com* les adresses 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 utiliser votre clé AWS KMS .

Si l'objet Amazon S3 est chiffré avec une AWS KMS clé, vous devez autoriser Amazon SES à utiliser la AWS KMS clé. 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'[CreateImportJob](#) opération dans l'API SES v2.

Note

L'exemple suivant suppose que vous avez déjà installé le 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](#).

En ligne de commande, entrez la commande suivante. **s3bucket** Remplacez-le 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 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 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 consulter la liste de toutes les adresses e-mail figurant sur la liste de suppression au niveau de votre compte en utilisant l'[ListSuppressedDestinations](#) opération de l'API SES v2.

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 inclut un champ « NextToken » avec une valeur de chaîne, cela indique que des adresses e-mail supplémentaires figurent sur 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 *string* par la NextToken valeur 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 par `1604394130` 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 par `1611126000` 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 (telle que 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 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 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 figure sur la liste de suppression de votre compte, mais que vous savez qu'elle ne devrait pas y figurer, vous pouvez la supprimer en utilisant l'[DeleteSuppressedDestination](#) opération dans l'API SES v2.

Pour supprimer des adresses individuelles de la liste de suppression au niveau de votre compte à l'aide du 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 du 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 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 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 masse en téléchargeant d'abord votre liste de contacts dans un objet Amazon S3, puis en utilisant l'[CreateImportJob](#) opération 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 par *recipient3@example.com* les adresses e-mail que vous souhaitez supprimer de la liste de suppression au niveau du 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.

- Autorisez SES à utiliser votre AWS KMS clé.

Si l'objet Amazon S3 est chiffré avec une AWS KMS clé, vous devez autoriser Amazon SES à utiliser la AWS KMS clé. 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'[CreateImportJob](#) opération dans l'API SES v2.

Note

L'exemple suivant suppose que vous avez déjà installé le 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](#).

En ligne de commande, entrez la commande suivante. *s3bucket* Remplacez-le 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 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 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 consulter la liste de toutes les adresses e-mail figurant sur la liste de suppression au niveau de votre compte en utilisant l'[ListImportJobs](#) opération de l'API Amazon SES v2.

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 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 **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 en utilisant l'[GetImportJob](#) opération de l'API Amazon SES v2.

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 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 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'[PutAccountSuppressionAttributes](#) opération de l'API SES v2 pour désactiver efficacement votre liste de suppression au niveau du compte en supprimant les valeurs de l'`suppressed-reasons` attribut.

Pour désactiver la liste de suppression au niveau de votre compte à l'aide du 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 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 Suppression list (Liste de suppression).
3. Dans le volet des Account-level paramètres, choisissez Modifier.
4. Dans Suppression list (Liste de suppression), décochez la case Enabled (Activé).
5. Sélectionnez Enregistrer les modifications.

Utilisation de listes de suppression au niveau des locataires dans Amazon SES

Si vous utilisez la solution mutualisée Amazon Simple Email Service (SES) pour envoyer des e-mails au nom de plusieurs locataires, vous pouvez attribuer à chaque locataire sa propre liste de suppression. Tenant-level la suppression isole les rebonds et les plaintes afin qu'ils n'affectent que le locataire qui a envoyé l'e-mail. Sans cette fonctionnalité, tous les locataires partagent la liste de suppression au niveau du compte. Lorsqu'un destinataire renvoie ou se plaint de l'adresse e-mail d'un locataire, cette adresse est supprimée pour tous les locataires du compte. Tenant-level

la suppression empêche cette contamination entre locataires en maintenant une liste distincte d'adresses supprimées pour chaque locataire.

Comment fonctionne la suppression au niveau des locataires

Deux paramètres contrôlent le comportement de suppression pour chaque locataire : l'étendue de la suppression et les raisons de la suppression. Vous configurez les deux paramètres ensemble en utilisant l'opération `PutTenantSuppressionAttributesAPI` ou en spécifiant à `SuppressionAttributes` quel moment vous créez un locataire avec l'opération `CreateTenant` d'API.

L'étendue de suppression détermine la liste de suppression utilisée par SES pour le locataire :

- **TENANT**— Utilisez la propre liste de suppression du locataire.
- **ACCOUNT**— Utilisez la liste de suppression au niveau du compte. Il s'agit de la valeur par défaut pour les locataires existants et nouveaux.

Les raisons supprimées déterminent les événements qui poussent SES à ajouter des adresses à la liste de suppression :

- **BOUNCE**— Ajoutez des adresses qui produisent des rebonds brusques.
- **COMPLAINT**— Ajoutez les adresses qui génèrent des plaintes.
- **BOUNCEet COMPLAINT** — Ajoutez les adresses qui produisent l'un ou l'autre événement.
- **Vide** : ne cochez ni n'inscrivez dans aucune liste de suppression.

Note

Vous devez fournir `SuppressionScope` et `SuppressedReasons` ensemble, ou définir les deux sur null. Le fait de définir les deux sur null efface les paramètres de suppression du locataire et rétablit le comportement d'**ACCOUNT** étendue par défaut du locataire.

Comportement de suppression par configuration

Le tableau suivant décrit l'heure d'envoi et le comportement d'enregistrement pour chaque combinaison d'étendue de suppression et de raisons de suppression.

Scope	Motifs	Send-time comportement	Comportement d'enregistrement
TENANT	BOUNCE, COMPLAINT	Vérifie la liste des locataires pour détecter les rebonds et les plaintes	Enregistre les deux dans la liste des locataires
TENANT	BOUNCE	Vérifie la liste des locataires pour les rebonds uniquement	Les enregistrements sont renvoyés à la liste des locataires uniquement
TENANT	COMPLAINT	Vérifie la liste des locataires pour les plaintes uniquement	Enregistre les plaintes adressées uniquement à la liste des locataires
TENANT	Vide	Aucun contrôle de suppression	Pas d'enregistrement
ACCOUNT	BOUNCE, COMPLAINT	Vérifie la liste des comptes pour détecter les rebonds et les plaintes	Enregistre les deux dans la liste des comptes
ACCOUNT	BOUNCE	Vérifie la liste des comptes pour les rebonds uniquement	Les enregistrements sont renvoyés à la liste des comptes uniquement
ACCOUNT	COMPLAINT	Vérifie la liste des comptes pour les plaintes uniquement	Enregistre les plaintes uniquement dans la liste des comptes
ACCOUNT	Vide	Aucun contrôle de suppression	Pas d'enregistrement

Priorité de suppression et comportement au moment de l'envoi

SES résout les paramètres de suppression dans l'ordre de priorité suivant, du plus élevé au plus bas :

1. Ensemble de configuration : si le jeu de configuration spécifie des paramètres de suppression, SES utilise ces paramètres.
2. Tenant — S'il n'existe aucune dérogation aux ensembles de configuration, SES utilise les paramètres de suppression du locataire.
3. Compte — Si ni le jeu de configuration ni le locataire ne spécifient de paramètres, SES utilise les valeurs par défaut au niveau du compte.

Important

L'étendue de suppression détermine la liste de suppression que SES vérifie au moment de l'envoi. Lorsque le périmètre est défini `TENANT`, SES vérifie uniquement la liste de suppression du locataire et ignore la liste de suppression au niveau du compte. Une adresse figurant sur la liste de suppression au niveau du compte mais pas sur la liste de suppression du locataire n'est pas supprimée. Lorsque le champ d'application est `ACCOUNT` défini, SES vérifie uniquement la liste de suppression au niveau du compte. Le scope contrôle également l'endroit où les rebonds et les plaintes sont enregistrés.

Dérogations des ensembles de configuration

Le set `SuppressionOptions` for a configuration inclut désormais un `SuppressionScope` champ. Vous pouvez utiliser un ensemble de configuration pour modifier le champ d'application uniquement, les raisons uniquement, ou les deux indépendamment. Cela vous permet de contrôler avec précision le comportement de suppression pour des flux de travail d'envoi spécifiques. Il n'est pas nécessaire de modifier les paramètres par défaut du locataire.

Enregistrement de suppression automatique

Lorsque le périmètre de suppression est défini `TENANT`, SES enregistre automatiquement les entrées de suppression comme suit :

- Hard bounces — SES ajoute l'adresse à la liste de suppression du locataire et à la liste de suppression globale. SES n'ajoute pas l'adresse à la liste de suppression au niveau du compte.
- Réclamations — SES ajoute l'adresse uniquement à la liste de suppression du locataire.
- Not-spam feedback — Lorsqu'un destinataire marque un message précédemment signalé comme n'étant pas du spam, SES supprime automatiquement les entrées `COMPLAINT` -reason de la liste de suppression du locataire.

Identifier les rebonds liés à la suppression des locataires

Lorsque SES supprime un message parce que l'adresse figure sur la liste de suppression d'un locataire, vous pouvez identifier l'événement à l'aide des indicateurs suivants :

- Notification de rebond — Le type de rebond comporte un Permanent sous-type de `OnTenantSuppressionList`
- Virtual Deliverability Manager (VDM) — La raison du rebond est que `ON_TENANT_SUPPRESSION_LIST`
- Code diagnostique — "Amazon SES did not send the message to this address because it is on the suppression list for your tenant."
- Tag d'événement : SES ajoute un `ses:tenant-name` tag aux notifications de rebond et de réclamation afin que vous puissiez identifier à quel locataire appartient l'événement.

Gestion des entrées de la liste de suppression des locataires

Vous gérez les entrées de la liste de suppression des locataires en utilisant les mêmes opérations d'API que celles que vous utilisez pour les entrées au niveau du compte. Pour cibler la liste de suppression d'un locataire, incluez le `TenantName` paramètre dans votre demande :

- `PutSuppressedDestination`— Ajoutez une adresse à la liste de suppression d'un locataire.
- `GetSuppressedDestination`— Récupère les détails d'une adresse supprimée pour un locataire.
- `DeleteSuppressedDestination`— Supprime une adresse de la liste de suppression d'un locataire.
- `ListSuppressedDestinations`— Répertoire toutes les adresses supprimées pour un locataire.

Si vous omettez le `TenantName` paramètre, ces opérations ciblent la liste de suppression au niveau du compte. Cela permet de maintenir la rétrocompatibilité avec les intégrations existantes.

Considérations et restrictions

Gardez les points suivants à l'esprit lorsque vous utilisez des listes de suppression au niveau des locataires :

- Multi-tenancy obligatoire — La mutualisation de SES doit être configurée avec au moins un locataire pour utiliser cette fonctionnalité.
- Une liste par locataire — Chaque locataire possède exactement une liste de suppression. Il existe un mappage 1:1 entre les locataires et les listes de suppression.
- Region-specific— Les listes de suppression de locataires sont spécifiques à Région AWS celles dans lesquelles vous les configurez.
- Les adresses persistent : les adresses supprimées restent sur la liste du locataire jusqu'à ce que vous les supprimiez explicitement ou jusqu'à ce que SES les supprime automatiquement (par exemple, lorsqu'un destinataire signale un événement de non-spam pour une entrée « COMPLAINT -reason »).
- Case-sensitive stockage — Les adresses e-mail figurant sur la liste de suppression sont stockées en majuscules et minuscules. Les appels d'API pour la gestion des listes de suppression nécessitent une correspondance entre les cas exacts.
- Impact du quota d'envoi : les messages supprimés par une liste de suppression de locataires sont pris en compte dans votre quota d'envoi quotidien.
- Données relatives aux plaintes Gmail : Gmail n'envoie pas de données relatives aux plaintes à SES. Les adresses hébergées par Gmail ne sont pas automatiquement ajoutées à la liste de suppression des plaintes.
- Restrictions relatives au bac à sable : vous ne pouvez pas appeler `PutSuppressedDestination` tant que votre compte ne dispose pas d'un accès à la production.
- Effacement des paramètres : pour effacer les paramètres de suppression d'un locataire, appelez `PutTenantSuppressionAttributes` avec des valeurs nulles pour des raisons d'étendue et pour des raisons.
- Supprimer un locataire : lorsque vous supprimez un locataire, SES supprime également toutes les entrées de la liste de suppression pour ce locataire.

Ressources connexes

Les ressources suivantes peuvent vous aider à en savoir plus sur les listes de suppression dans SES.

- [Utilisation de la liste de suppression au niveau du compte Amazon SES](#)
- [Liste de suppression globale Amazon SES](#)

Configuration de la suppression au niveau du locataire

Configurez les paramètres de suppression au niveau du locataire pour contrôler la manière dont Amazon Simple Email Service (Amazon SES) gère les rebonds et les plaintes des locataires individuels. Par défaut, les locataires utilisent votre liste de suppression au niveau du compte. Lorsque vous activez la suppression au niveau du locataire, SES gère une liste de suppression distincte pour chaque locataire. Cela vous permet de contrôler de manière granulaire la délivrabilité des e-mails.

Cette rubrique décrit les procédures permettant d'activer, de modifier, de désactiver et d'afficher les paramètres de suppression au niveau du locataire à l'aide du AWS CLI

Important

La désactivation de la suppression au niveau du locataire ne supprime pas les entrées existantes de la liste de suppression du locataire. Si vous réactivez la suppression au niveau du locataire ultérieurement, ces entrées sont toujours actives.

Conditions préalables

Avant de configurer la suppression au niveau du locataire, assurez-vous que vous répondez aux exigences suivantes :

- Multi-tenancy est activé dans votre compte SES.
- Au moins un locataire existe dans votre compte, ou vous prévoyez d'en créer un dans le cadre de cette procédure.
- AWS CLI la version 2 est installée et configurée avec les autorisations appropriées. Pour plus d'informations, consultez le [Guide de l'utilisateur AWS Command Line Interface](#).
- Vous connaissez les concepts de suppression au niveau du compte. Pour de plus amples informations, veuillez consulter [Utilisation de la liste de suppression au niveau du compte Amazon SES](#).

Activation de la suppression au niveau du locataire pour un locataire existant

Utilisez l'opération `PutTenantSuppressionAttributes` API pour activer la suppression au niveau du locataire pour un locataire existant. Cette opération est idempotente, vous pouvez donc l'appeler plusieurs fois avec les mêmes paramètres sans effets secondaires.

Pour activer la suppression au niveau du locataire

1. Sur la ligne de commande, exécutez la `put-tenant-suppression-attributes` commande suivante pour activer la suppression au niveau du locataire à la fois pour les rebonds et les plaintes :

Linux, macOS, or Unix

```
aws sesv2 put-tenant-suppression-attributes \  
--tenant-name MyTenant \  
--suppression-scope TENANT \  
--suppressed-reasons BOUNCE COMPLAINT
```

Windows

```
aws sesv2 put-tenant-suppression-attributes `\  
--tenant-name MyTenant `\  
--suppression-scope TENANT `\  
--suppressed-reasons BOUNCE COMPLAINT
```

Remplacez *MyTenant* par le nom de votre locataire.

2. Vérifiez que la commande ne renvoie aucune sortie. Une requête réussie renvoie une réponse HTTP 200 sans corps.
3. Confirmez la configuration en exécutant la commande suivante :

```
aws sesv2 get-tenant --tenant-name MyTenant
```

Le locataire utilise désormais sa propre liste de suppression pour les rebonds et les plaintes.

Vous pouvez également configurer la suppression pour un seul type de raison. Les exemples suivants montrent comment activer la suppression pour les rebonds uniquement ou pour les plaintes uniquement.

La commande suivante supprime uniquement les rebonds :

Linux, macOS, or Unix

```
aws sesv2 put-tenant-suppression-attributes \  
--tenant-name MyTenant \  
--suppression-scope BOUNCE
```

```
--tenant-name MyTenant \  
--suppression-scope TENANT \  
--suppressed-reasons BOUNCE
```

Windows

```
aws sesv2 put-tenant-suppression-attributes \  
--tenant-name MyTenant \  
--suppression-scope TENANT \  
--suppressed-reasons BOUNCE
```

La commande suivante supprime uniquement les plaintes :

Linux, macOS, or Unix

```
aws sesv2 put-tenant-suppression-attributes \  
--tenant-name MyTenant \  
--suppression-scope TENANT \  
--suppressed-reasons COMPLAINT
```

Windows

```
aws sesv2 put-tenant-suppression-attributes \  
--tenant-name MyTenant \  
--suppression-scope TENANT \  
--suppressed-reasons COMPLAINT
```

Note

Vous devez fournir `--suppression-scope` et `--suppressed-reasons` ensemble. Fournir l'un sans l'autre renvoie un `InvalidParameterValueException`.

Configuration de la suppression lors de la création d'un nouveau locataire

Utilisez l'opération `CreateTenant` API avec le `SuppressionAttributes` paramètre pour créer un locataire avec la suppression au niveau du locataire activée dès le départ.

Pour créer un locataire avec suppression au niveau du locataire

1. Sur la ligne de commande, exécutez la `create-tenant` commande suivante :

Linux, macOS, or Unix

```
aws sesv2 create-tenant \  
--tenant-name MyNewTenant \  
--suppression-attributes '{"SuppressionScope":"TENANT","SuppressedReasons":  
["BOUNCE","COMPLAINT"]}'
```

Windows

```
aws sesv2 create-tenant \  
--tenant-name MyNewTenant \  
--suppression-attributes '{"SuppressionScope":"TENANT","SuppressedReasons":  
["BOUNCE","COMPLAINT"]}'
```

Remplacez *MyNewTenant* par le nom de votre nouveau locataire.

2. Vérifiez que la réponse contient l'ID du locataire :

```
{  
  "TenantId": "tn-abc123def456"  
}
```

Le locataire est créé avec la suppression au niveau du locataire activée à la fois pour les rebonds et les plaintes.

Note

Si vous omettez `--suppression-attributes`, le locataire utilise par défaut le `ACCOUNT` champ d'application et utilise la liste de suppression au niveau du compte.

Remplacer la suppression des locataires par un ensemble de configuration

Vous pouvez annuler les paramètres de suppression d'un locataire en ajoutant ceux `SuppressionScope` d'un ensemble de `SuppressionOptions` configuration. Lorsque vous

envoyez un e-mail à l'aide de ce jeu de configuration, les paramètres de suppression du jeu de configuration ont priorité sur les paramètres du locataire. Vous pouvez modifier le champ d'application uniquement, les raisons uniquement, ou les deux indépendamment.

Pour créer un ensemble de configuration avec remplacement de l'étendue du locataire

1. Sur la ligne de commande, exécutez la `create-configuration-set` commande suivante :

Linux, macOS, or Unix

```
aws sesv2 create-configuration-set \  
--configuration-set-name my-config-set \  
--suppression-options '{"SuppressionScope":"TENANT","SuppressedReasons":  
["BOUNCE"]}'
```

Windows

```
aws sesv2 create-configuration-set \  
--configuration-set-name my-config-set \  
--suppression-options '{"SuppressionScope":"TENANT","SuppressedReasons":  
["BOUNCE"]}'
```

my-config-set Remplacez-le par le nom de votre ensemble de configuration.

2. Vérifiez que la commande ne renvoie aucune sortie. Une requête réussie renvoie une réponse HTTP 200.

Pour mettre à jour un ensemble de configuration existant avec des options de suppression

1. Sur la ligne de commande, exécutez la `put-configuration-set-suppression-options` commande suivante :

Linux, macOS, or Unix

```
aws sesv2 put-configuration-set-suppression-options \  
--configuration-set-name my-config-set \  
--suppression-scope TENANT \  
--suppressed-reasons BOUNCE
```

Windows

```
aws sesv2 put-configuration-set-suppression-options `
--configuration-set-name my-config-set `
--suppression-scope TENANT `
--suppressed-reasons BOUNCE
```

my-config-set Remplacez-le par le nom de votre ensemble de configuration.

2. Vérifiez que la commande ne renvoie aucune sortie. Une requête réussie renvoie une réponse HTTP 200.

Désactivation de la suppression au niveau du locataire

Pour rétablir la suppression au niveau du compte pour un locataire, vous pouvez définir l'étendue ACCOUNT ou effacer tous les paramètres de suppression.

Pour configurer le locataire pour une suppression au niveau du compte

1. Sur la ligne de commande, exécutez la commande suivante pour définir explicitement la portée sur ACCOUNT :

Linux, macOS, or Unix

```
aws sesv2 put-tenant-suppression-attributes \
--tenant-name MyTenant \
--suppression-scope ACCOUNT \
--suppressed-reasons BOUNCE COMPLAINT
```

Windows

```
aws sesv2 put-tenant-suppression-attributes `
--tenant-name MyTenant `
--suppression-scope ACCOUNT `
--suppressed-reasons BOUNCE COMPLAINT
```

Remplacez *MyTenant* par le nom de votre locataire.

2. Vérifiez que la commande ne renvoie aucune sortie.

Pour effacer tous les paramètres de suppression

1. Sur la ligne de commande, exécutez la commande suivante sans préciser le champ d'application ni les raisons :

```
aws sesv2 put-tenant-suppression-attributes --tenant-name MyTenant
```

Remplacez *MyTenant* par le nom de votre locataire.

2. Vérifiez que la commande ne renvoie aucune sortie.

Note

Lorsque vous omettez les deux `--suppression-scope` et `--suppressed-reasons`, SES efface les paramètres de suppression du locataire. Le locataire adopte un comportement de suppression au niveau du compte.

Important

La désactivation de la suppression au niveau du locataire ne supprime pas les entrées existantes de la liste de suppression du locataire. Si vous réactivez la suppression au niveau du locataire ultérieurement, ces entrées sont toujours actives.

Affichage de la configuration de suppression actuelle

Utilisez l'opération `GetTenant` API pour vérifier les paramètres de suppression actuels d'un locataire.

Pour consulter la configuration de suppression d'un locataire

1. Sur la ligne de commande, exécutez la `get-tenant` commande suivante :

```
aws sesv2 get-tenant --tenant-name MyTenant
```

Remplacez *MyTenant* par le nom de votre locataire.

2. Passez en revue la réponse. L'exemple suivant montre un locataire pour lequel la suppression au niveau du locataire est activée :

```
{
  "Tenant": {
    "TenantName": "MyTenant",
    "TenantId": "tn-abc123def456",
    "TenantArn": "arn:aws:ses:us-east-1:123456789012:tenant/MyTenant/tn-abc123def456",
    "SendingStatus": "ENABLED",
    "CreatedTimestamp": 1705312800,
    "UpdateTimestamp": 1705762800,
    "SuppressionAttributes": {
      "SuppressionScope": "TENANT",
      "SuppressedReasons": ["BOUNCE", "COMPLAINT"]
    }
  }
}
```

Le tableau suivant décrit les principaux champs de l'`SuppressionAttributes` objet.

Champ	Description
<code>SuppressionScope</code>	L'étendue de la suppression pour le locataire. La valeur de <code>TENANT</code> signifie que le locataire utilise sa propre liste de suppression. La valeur de <code>ACCOUNT</code> signifie que le locataire utilise la liste de suppression au niveau du compte.
<code>SuppressedReasons</code>	Les raisons de suppression actives pour le locataire. Les valeurs possibles sont <code>BOUNCE</code> , <code>COMPLAINT</code> , ou les deux.

En cas `SuppressionAttributes` d'absence ou de valeur nulle dans la réponse, le locataire utilise la suppression au niveau du compte.

Résolution des problèmes

Les erreurs suivantes sont courantes que vous pouvez rencontrer lors de la configuration de la suppression au niveau du locataire.

`InvalidParameterValueException: SuppressedReasons cannot be null when SuppressionScope is provided`

- Cause — Vous avez spécifié `--suppression-scope` sans `--suppressed-reasons`.
- Corriger — Fournissez les deux paramètres ensemble, ou omettez les deux pour effacer les paramètres.

`InvalidParameterValueException: SuppressionScope is required when SuppressedReasons are provided`

- Cause — Vous avez spécifié `--suppressed-reasons` sans `--suppression-scope`.
- Corriger — Fournissez les deux paramètres ensemble.

`NotFoundException`

- Cause — Le nom du locataire que vous avez spécifié n'existe pas.
- Correctif — Vérifiez le nom du locataire en exécutant la commande suivante :

```
aws sesv2 list-tenants
```

Ressources connexes

- [Utilisation de listes de suppression au niveau des locataires dans Amazon SES](#)
- [Gestion des entrées de la liste de suppression des locataires](#)
- [Utilisation de la liste de suppression au niveau du compte Amazon SES](#)
- [Locataires](#)

Gestion des entrées de la liste de suppression des locataires

Vous gérez les entrées sur la liste de suppression d'un locataire en utilisant les mêmes opérations d'API Amazon Simple Email Service (SES) que celles que vous utilisez pour la liste de suppression au niveau du compte. Pour cibler la liste d'un locataire spécifique, incluez le `--tenant-name` paramètre dans chaque demande. Lorsque vous omettez ce paramètre, les opérations ciblent la liste au niveau du compte. Utilisez le AWS CLI pour ajouter, vérifier, supprimer et répertorier les adresses supprimées pour un locataire spécifique.

⚠ Important

Les adresses e-mail figurant sur la liste de suppression sont conservées en majuscules et minuscules. Alors que la fonctionnalité d'envoi d'e-mails traite les adresses présentant des cas différents comme identiques, les appels d'API pour la gestion des listes de suppression nécessitent une correspondance exacte entre les cas. Assurez-vous d'utiliser la majuscule exacte de l'adresse e-mail telle qu'elle apparaît dans la liste de suppression lorsque vous ajoutez, vérifiez ou supprimez des entrées.

Conditions préalables

Avant de gérer les entrées de la liste de suppression de locataires, assurez-vous que vous répondez aux exigences suivantes :

- Tenant-level la suppression est activée pour le locataire. Pour de plus amples informations, veuillez consulter [Configuration de la suppression au niveau du locataire](#).
- AWS CLI la version 2 est installée et configurée avec les autorisations appropriées. Pour plus d'informations, consultez le [Guide de l'utilisateur AWS Command Line Interface](#).
- Le locataire existe dans votre compte SES.

Ajouter une adresse à la liste de suppression d'un locataire

Utilisez l'opération `PutSuppressedDestination` API avec le `--tenant-name` paramètre pour ajouter une adresse e-mail à la liste de suppression d'un locataire.

Pour ajouter une adresse à la liste de suppression d'un locataire à l'aide du 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 \  
--tenant-name MyTenant
```

Windows

```
aws sesv2 put-suppressed-destination `
--email-address recipient@example.com `
--reason BOUNCE `
--tenant-name MyTenant
```

Dans l'exemple précédent, remplacez *recipient@example.com* par l'adresse e-mail à ajouter, *BOUNCE* par le motif de suppression (les valeurs acceptables sont BOUNCE et COMPLAINT) et *MyTenant* par le nom de votre locataire.

La commande ne produit aucun résultat en cas de succès (HTTP 200). L'adresse figure désormais sur la liste de suppression du locataire.

Note

Le `--reason` paramètre accepte BOUNCE ou COMPLAINT. Vous pouvez ajouter la même adresse pour différentes raisons.

Vérifier si une adresse figure sur la liste de suppression d'un locataire

Utilisez l'opération `GetSuppressedDestination` API avec le `--tenant-name` paramètre pour vérifier si une adresse e-mail figure sur la liste de suppression d'un locataire.

Pour vérifier si une adresse figure sur la liste de suppression d'un locataire à l'aide du AWS CLI

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

Linux, macOS, or Unix

```
aws sesv2 get-suppressed-destination \
--email-address recipient@example.com \
--tenant-name MyTenant
```

Windows

```
aws sesv2 get-suppressed-destination `
```

```
--email-address recipient@example.com `
--tenant-name MyTenant
```

Dans l'exemple précédent, remplacez *recipient@example.com* par l'adresse e-mail à vérifier et *MyTenant* par le nom de votre locataire.

Si l'adresse figure sur la liste de suppression du locataire, la commande renvoie un résultat semblable à l'exemple suivant :

```
{
  "SuppressedDestination": {
    "EmailAddress": "recipient@example.com",
    "Reason": "BOUNCE",
    "LastUpdateTime": "2026-03-15T10:30:00.000Z",
    "Attributes": {
      "MessageId": "0100018e1234abcd-12345678-abcd-1234-
abcd-123456789012-000000",
      "FeedbackId": "0100018e1234abce-12345678-abcd-1234-
abcd-123456789012-000000"
    }
  }
}
```

La réponse inclut les champs suivants :

- **EmailAddress**— L'adresse e-mail supprimée.
- **Reason**— Pourquoi l'adresse a été supprimée (BOUNCE ou COMPLAINT).
- **LastUpdateTime**— Date de dernière mise à jour de l'entrée.
- **Attributes**— Contient MessageId et FeedbackId provient de l'événement à l'origine de la suppression. Ces champs sont présents pour les adresses supprimées automatiquement et absents pour les entrées ajoutées manuellement.

Note

Si l'adresse ne figure pas sur la liste de suppression du locataire, l'API renvoie `unNotFoundException`.

Supprimer une adresse de la liste de suppression d'un locataire

Utilisez l'opération `DeleteSuppressedDestination` API avec le `--tenant-name` paramètre pour supprimer une adresse e-mail de la liste de suppression d'un locataire.

Pour supprimer une adresse de la liste de suppression d'un locataire à l'aide du 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 \  
--tenant-name MyTenant
```

Windows

```
aws sesv2 delete-suppressed-destination `\  
--email-address recipient@example.com `\  
--tenant-name MyTenant
```

Dans l'exemple précédent, remplacez *recipient@example.com* par l'adresse e-mail à supprimer et *MyTenant* par le nom de votre locataire.

La commande ne produit aucun résultat en cas de succès (HTTP 200). L'adresse est supprimée de la liste de suppression du locataire.

Important

La suppression d'une adresse de la liste de suppression d'un locataire ne la supprime pas de la liste de suppression globale ou de la liste de suppression au niveau du compte. Chaque liste est gérée de manière indépendante.

Inscrire des adresses sur la liste de suppression d'un locataire

Utilisez l'opération `ListSuppressedDestinations` API avec le `--tenant-name` paramètre pour récupérer toutes les adresses supprimées pour un locataire spécifique.

Pour répertorier toutes les adresses figurant sur la liste de suppression d'un locataire à l'aide du AWS CLI

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

Linux, macOS, or Unix

```
aws sesv2 list-suppressed-destinations \  
--tenant-name MyTenant
```

Windows

```
aws sesv2 list-suppressed-destinations `\  
--tenant-name MyTenant
```

Dans l'exemple précédent, remplacez *MyTenant* par le nom de votre locataire.

L'exemple de sortie suivant montre deux adresses supprimées :

```
{  
  "SuppressedDestinationSummaries": [  
    {  
      "EmailAddress": "bounce@example.com",  
      "Reason": "BOUNCE",  
      "LastUpdateTime": "2026-03-10T08:15:00.000Z"  
    },  
    {  
      "EmailAddress": "complaint@example.com",  
      "Reason": "COMPLAINT",  
      "LastUpdateTime": "2026-03-12T14:30:00.000Z"  
    }  
  ]  
}
```

Filtrer les résultats

Vous pouvez filtrer les résultats par raison, par plage de dates ou par les deux.

La commande suivante filtre par raison :

Linux, macOS, or Unix

```
aws sesv2 list-suppressed-destinations \  
--tenant-name MyTenant \  
--reasons BOUNCE COMPLAINT
```

Windows

```
aws sesv2 list-suppressed-destinations `\  
--tenant-name MyTenant `\  
--reasons BOUNCE COMPLAINT
```

La commande suivante filtre par plage de dates :

Linux, macOS, or Unix

```
aws sesv2 list-suppressed-destinations \  
--tenant-name MyTenant \  
--start-date 2026-01-01T00:00:00Z \  
--end-date 2026-03-31T23:59:59Z
```

Windows

```
aws sesv2 list-suppressed-destinations `\  
--tenant-name MyTenant `\  
--start-date 2026-01-01T00:00:00Z `\  
--end-date 2026-03-31T23:59:59Z
```

Si la réponse inclut une `NextToken` valeur, utilisez-la dans une demande ultérieure pour obtenir d'autres résultats. Utilisez le `--page-size` paramètre pour contrôler le nombre de résultats par page.

Note

L'opération de liste renvoie uniquement des informations récapitulatives. Pour obtenir tous les détails `Attributes`, y compris, utilisez `GetSuppressedDestination` les adresses individuelles.

Entrées de suppression automatique

SES gère automatiquement les entrées de suppression en fonction de la configuration de suppression du locataire. Vous n'avez aucune action à effectuer pour les saisies automatiques. Ils apparaissent dans la liste de suppression du locataire à côté des entrées ajoutées manuellement.

SES ajoute automatiquement des entrées dans les cas suivants :

- Un rebond dur se produit si la suppression du rebond est activée pour le locataire.
- Une plainte est reçue si la suppression de la plainte est activée pour le locataire.

SES supprime automatiquement les entrées dans les cas suivants :

- Un rapport de non-spam est reçu pour une adresse dont la plainte a été supprimée.

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.

Si vous utilisez le multitenant, les ensembles de configuration peuvent également remplacer les paramètres de suppression au niveau du locataire. L'ensemble de configuration `SuppressionOptions` pour un ensemble de configuration inclut un `SuppressionScope` champ qui détermine la liste de suppression utilisée par SES. Vous pouvez configurer `SuppressionScope` `TENANT` pour utiliser la liste de suppression du locataire ou `ACCOUNT` pour utiliser la liste de

suppression au niveau du compte. Vous pouvez modifier le champ d'application, les raisons supprimées ou les deux indépendamment. Pour plus d'informations sur la suppression au niveau du locataire, consultez. [Utilisation de listes de suppression au niveau des locataires dans Amazon SES](#)

 Important

Si vous définissez `SuppressionScope` un ensemble de configuration, toutes `SendEmail` les `SendBulkEmail` demandes utilisant ce jeu de configuration doivent inclure un nom de locataire. TENANT Les demandes sans nom de locataire sont rejetées.

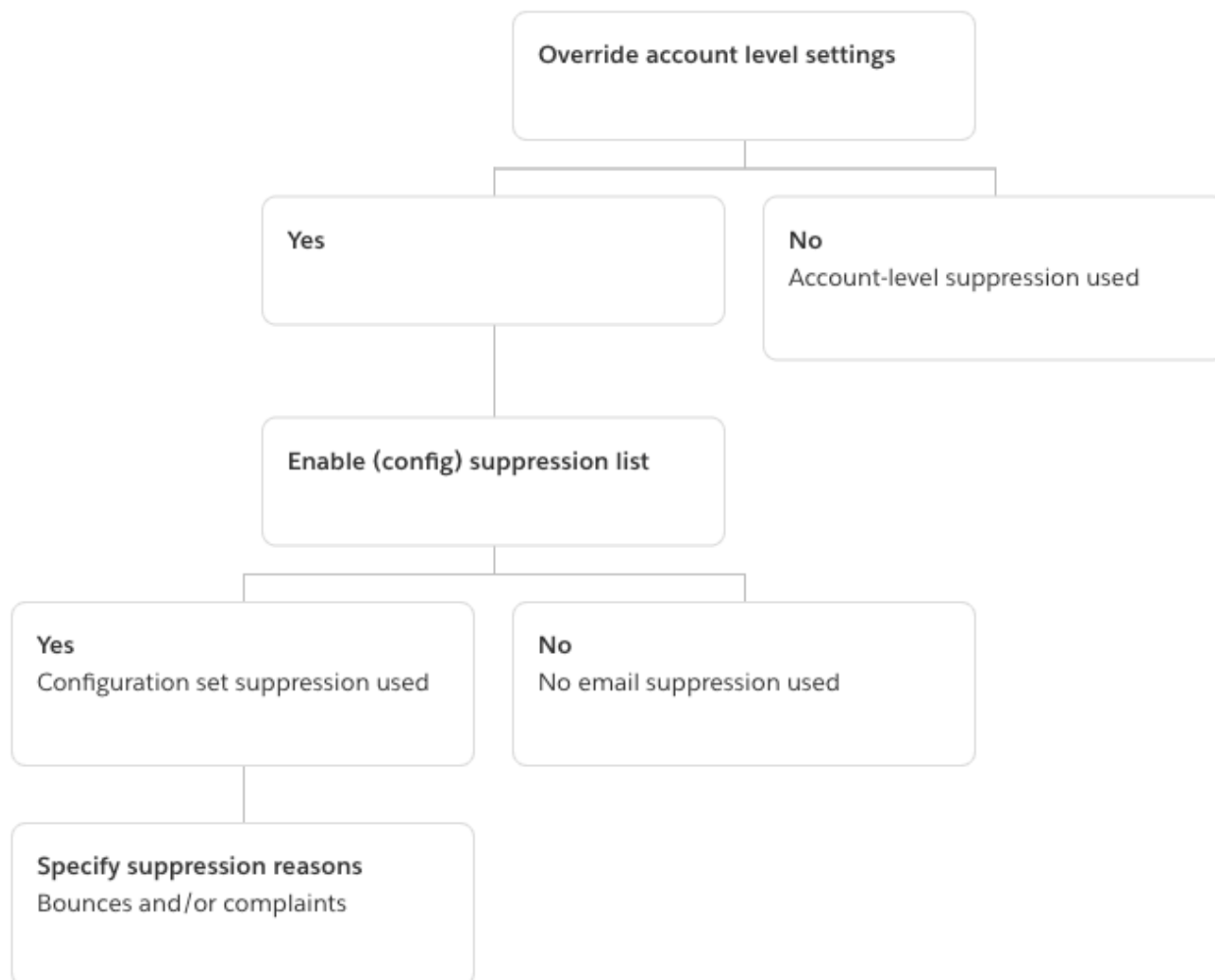
Avec la suppression au niveau du jeu de configurations, il existe différents niveaux de suppression au niveau du compte, y compris la possibilité de ne pas utiliser de suppression du tout. Pour aider à comprendre ces différents niveaux de suppression qui peuvent être définis dans les procédures de console 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.

 Note

Pour toute condition de suppression non spécifiée au niveau de l'ensemble de configuration, le comportement de suppression reviendra à la liste de suppression globale puisque les paramètres au niveau du compte ont été remplacés.

Configuration set-level suppression logic



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 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. 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. Sélectionnez 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 SES à l'aide de l'[CreateImportJob](#) API.
- SES émettra un événement de rebond pour un message 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'[CreateContactList](#) opération dans l'API SES v2 pour créer une liste de contacts. Vous pouvez configurer rapidement et facilement ce paramètre en utilisant 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 une liste de contacts à l'aide du 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 d'accès au fichier JSON pour votre [CreateContactList](#) demande.

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'[CreateContact](#) opération dans l'API SES v2 pour créer un contact. Vous pouvez configurer rapidement et facilement ce paramètre en utilisant 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 un contact à l'aide du 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 d'accès au fichier JSON pour votre [CreateContact](#) demande.

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 masse en téléchargeant d'abord vos contacts dans un objet Amazon S3, puis en utilisant l'[CreateImportJob](#) opération de l'API SES v2 ou en utilisant la console SES. Pour de plus amples informations, veuillez consulter [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 1 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. De plus, remplacez *Sports* et *Cycling* par celui *topicName* qui s'applique à votre contact. Les acceptables *topicPreferences* 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 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.

- Autorisez SES à utiliser votre AWS KMS clé.

Si l'objet Amazon S3 est chiffré à l'aide d'une AWS KMS clé, vous devez autoriser Amazon SES à utiliser la clé 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 autoriser SES à utiliser la clé gérée par le client en ajoutant une déclaration 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'[CreateImportJob](#) opération dans l'API SES v2.

Note

L'exemple suivant suppose que vous avez déjà installé le 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](#).

En ligne de commande, entrez la commande suivante. *s3bucket* Remplacez-le 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. Répertoriez les contacts à l'aide du AWS CLI— Vous pouvez utiliser l'[ListContacts](#) opération pour récupérer la liste de tous vos contacts abonnés à un sujet particulier, en conjonction avec l'[SendEmail](#) opération, 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 d'accès au fichier JSON pour votre [ListContacts](#) demande.

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 (`topicName` est 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.

SES émettra un événement de rebond pour un message envoyé à un contact désabonné de votre liste de contacts, ce qui signifie que vous n'aurez pas besoin de mettre à jour vos `SendEmail` demandes pour éviter de les envoyer à des contacts qui se sont désabonnés.

- Indiquez l'emplacement de vos liens de désabonnement — Lorsque vous les utilisez, [ListManagementOptions](#) vous avez la possibilité d'autoriser SES à ajouter des liens de bas de page de désabonnement dans votre e-mail en utilisant l'`{amazonSESUnsubscribeUrl}` espace réservé pour spécifier où SES doit insérer l'URL de désinscription. 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'`{{amazonSESUnsubscribeUrl}}` espace réservé ne peut être utilisé que s'il [ListManagementOptions](#) est spécifié comme en-tête lors de l'utilisation de l'[SendEmail](#) opération ou si X-SES-LIST-MANAGEMENT -OPTIONS est spécifié comme 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 ne sont inclus que lorsque SES n'essaie plus de livrer l'e-mail. En général, ces rebonds souples indiquent un échec de livraison, bien que dans

certains cas, un rebond souple puisse être renvoyé même lorsque le courrier parvient avec succès dans la boîte de réception du destinataire. Cela se produit généralement lorsque le destinataire envoie une réponse out-of-office automatique. Pour en savoir plus sur les soft bounces, consultez cet article de [AWS Re:Post](#).)

- **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 que vous souhaitez surveiller, de la granularité et du niveau de détail avec lesquels vous souhaitez que SES publie 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 SES	État du compte, e-mails envoyés, quota utilisé, demandes d'envoi réussies, rejets, rebonds et réclamations (historique	Page du tableau de bord du compte dans la console SES	Compte et pourcentage	Sur l'ensemble du AWS compte

Méthode de surveillance	Événements que vous pouvez surveiller	Méthode d'accès aux données	Niveau de détail	Granularité
	récent jusqu'à la réputation actuelle)			
Console SES	État du compte, e-mails envoyés, rebonds et réclamations (réputation actuelle)	Page de statistiques de réputation dans la console SES	Taux calculés uniquement	Sur l'ensemble du AWS compte
Virtual Deliverability Manager	Statistiques des comptes, fournisseur d'accès Internet, identités d'envoi, ensembles de configuration, envoi, livraison, plaintes, rebonds transitoires et permanents, ouvertures et clics, délivrabilité et réputation.	the section called "Tableau de bord" dans la console SES the section called "Conseiller" dans la console SES	Compte et pourcentage	Sur l'ensemble du AWS compte
UTILISER L'API	Messages délivrés, retours à l'expéditeur, réclamations et rejets	GetSendStatistics Opération d'API	Nombre uniquement	Sur l'ensemble du AWS compte

Méthode de surveillance	Événements que vous pouvez surveiller	Méthode d'accès aux données	Niveau de détail	Granularité
CloudWatch Console Amazon	Envois, livraisons, ouvertures, clics, rebonds, taux de rebond, plaintes, taux de réclamations, rejets, échecs de rendu et liste noire. IPs	CloudWatch console  Note Certaines mesures n'apparaissent pas dans 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	Sur l'ensemble du AWS compte

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). Consultez Configuration des notifications d'événement par e-mail.	Détails sur chaque événement	Sur l'ensemble du AWS compte

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. Cet écart peut être dû à des rebonds et à des rejets d'e-mails, ou à l'utilisation du simulateur de boîte de réception 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 des indicateurs de réputation : taux de rebond et de plaintes basés sur les dernières données obtenues lors du calcul de votre moyenne historique globale à un niveau élevé (il ne faut pas le confondre avec votre bounce/complaint taux normal, qui correspond à des bounce/complaint événements précis tels qu'ils se produisent en temps réel, comme indiqué sur la page du 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 $\text{Rejects/Sends} * 100$ 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 contient un CloudWatch bouton **Afficher** dans qui ouvre la métrique correspondante dans la CloudWatch console Amazon, ce qui permet de consulter des données détaillées, d'effectuer des calculs métriques personnalisés et [de créer des alarmes 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 console Amazon SES AWS Management Console et ouvrez-la 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 tous les graphiques, cliquez sur le CloudWatch bouton Afficher dans pour ouvrir la métrique correspondante dans la CloudWatch console Amazon où vous pouvez consulter des données détaillées, effectuer des calculs métriques personnalisés et [créer des alarmes de surveillance 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 l'un ou l'autre des volets, cliquez sur le CloudWatch bouton Afficher dans pour ouvrir la métrique correspondante dans la CloudWatch console Amazon où vous pouvez consulter des données détaillées, effectuer des calculs métriques personnalisés et [créer des alarmes de surveillance](#). 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 `GetSendStatistics` d'API à l'aide du AWS CLI”](#)
- [the section called “Appel de l'opération `GetSendStatistics` par programmation”](#)

Appel de l'opération **GetSendStatistics** d'API à l'aide du 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 **GetSendStatistics** d'API à l'aide du AWS CLI

1. Si vous ne l'avez pas déjà fait, installez l'AWS CLI. Pour plus d'informations, reportez-vous à la section « [Installation du AWS Command Line Interface](#) » dans le guide de AWS Command Line Interface l'utilisateur.

2. Si ce n'est pas déjà fait, configurez le AWS CLI pour utiliser vos AWS informations d'identification. Pour plus d'informations, reportez-vous à [la section « Configuration du AWS CLI »](#) dans le guide de AWS Command Line Interface l'utilisateur.
3. Dans la ligne de commande, exécutez la commande suivante :

```
aws ses get-send-statistics
```

Si le AWS CLI est correctement configuré, vous pouvez voir une liste des statistiques d'envoi au format JSON. 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'GetSendStatisticsopération à l'aide du AWS SDKs. Cette section inclut des exemples de code AWS SDKs 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 pour Go](#)
- [Exemple de code pour le kit AWS SDK pour PHP](#)
- [Exemple de code pour le kit AWS SDK pour Python \(Boto\)](#)
- [Exemple de code pour le kit AWS SDK pour Ruby](#)

Note

Ces exemples de code supposent que vous avez créé un fichier d'informations d'identification AWS partagé contenant votre identifiant de clé d' AWS accès, votre clé d'accès AWS secrète et votre AWS région préférée. Pour de plus amples informations, veuillez consulter [Informations d'identification et fichiers de configuration partagés](#).

Téléphoner **GetSendStatistics** à l'aide du AWS SDK pour 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)
}
```

Téléphoner **GetSendStatistics** à l'aide du AWS SDK pour 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";
}

?>
```

Téléphoner **GetSendStatistics** à l'aide du AWS SDK pour 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))
```

Téléphoner **GetSendStatistics** à l'aide du AWS SDK pour 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, Amazon Simple Notification Service ou EventBridge Amazon 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 envoyez un e-mail, vous fournissez le nom du jeu de configuration et une ou plusieurs balises de message, sous forme de name/value paires, pour 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 configurations, consultez [Utilisation des jeux de configuration dans Amazon SES](#).

Outre les balises de message que vous spécifiez, SES ajoute également 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 automatiques qui sont automatiquement appliquées aux messages que vous envoyez à l'aide de SES.

Balises automatiques SES

Nom de balise automatique	Description
<code>ses:caller-identity</code>	L'identité IAM de l'utilisateur SES qui a envoyé l'e-mail.
<code>ses:configuration-set</code>	Nom du jeu de configurations associé à l'e-mail.
<code>ses:from-domain</code>	Domaine de l'adresse de l'expéditeur.
<code>ses:outgoing-ip</code>	Adresse IP utilisée par SES pour envoyer l'e-mail.
<code>ses:source-ip</code>	Adresse IP que l'appelant a utilisée pour envoyer l'e-mail.

Nom de balise automatique	Description
<code>ses:source-tls-version</code>	Version du protocole TLS que l'appelant a utilisée pour envoyer l'e-mail.
<code>ses:outgoing-tls-version</code>	Version du protocole TLS utilisée par SES 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`-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`-tête est composé de l'identifiant, l'`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 SES.

- [Configuration de la publication d'événements](#)

- [Utilisation des données d'événement](#)

Terminologie de publication d'événements

La liste suivante définit les termes relatifs à la publication d'événements SES.

Événement d'envoi d'e-mail

Informations associées au résultat d'un e-mail que vous avez envoyé à 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 ne sont inclus que lorsque SES n'essaie plus de livrer l'e-mail. En général, ces rebonds souples indiquent un échec de livraison, bien que dans certains cas, un rebond souple puisse être renvoyé même lorsque le courrier parvient avec succès dans la boîte de réception du destinataire. Cela se produit généralement lorsque le destinataire envoie une réponse out-of-office automatique. Pour en savoir plus sur les soft bounces, consultez cet article de [AWS Re:Post](#).)
- **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 qui définit la destination vers laquelle SES publie les événements d'envoi d'e-mails, ainsi que 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 vers lequel vous publiez des événements d'envoi d'e-mails SES. Chaque destination d'événement que vous configurez appartient à un, et à un seul, jeu de configurations.

Balise de message

Une name/value paire que vous utilisez pour classer un e-mail dans le but de publier un événement. Par exemple, `campagne/livre` et `campagne/vêtements`. Lorsque vous envoyez un e-mail, vous spécifiez la balise du message en tant que paramètre de l'appel d'API ou en tant qu'en-tête d'e-mail spécifique à SES.

Balise automatique

Balises de messages qui sont automatiquement incluses dans les rapports de publication d'événements. Il existe un tag automatique pour le nom du jeu de configuration, le domaine de l'adresse « From », l'adresse IP sortante de l'appelant, l'adresse IP sortante SES et l'identité IAM de l'appelant.

Configuration de la publication d'événements Amazon SES

Cette section décrit ce que vous devez faire pour configurer Amazon SES afin de publier vos événements d'envoi d'e-mails aux AWS services 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](#)
- [Étape 2 : Ajout d'une destination d'événement](#)
- [Étape 3 : Spécifier votre jeu de configuration lorsque vous envoyez un e-mail](#)

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 ensembles de configuration à l'aide de l'[CreateConfigurationSet](#) opération de l'API Amazon SES V2 ou de l'Amazon SES CLI v2, voir [Créez un ensemble de configuration \(AWS CLI\)](#).

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 la destination d'un 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 de chaque type d'événement (par exemple, pour pouvoir définir le déclenchement d'une alarme lorsque le total devient trop élevé), utilisez 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. Étant donné qu'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 name/value paire qui vous permet d'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

- [Ajouter une destination CloudWatch d'événement](#)
- [Choix des CloudWatch dimensions](#)

Ajouter une destination CloudWatch d'événement

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 dans [Création d'une destination d'événement](#).

Vous pouvez également utiliser l'[UpdateConfigurationSetEventDestination](#) opération 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 précédentes [Création 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. Pour Dimension Name (Nom de la dimension), tapez le nom de la dimension que vous souhaitez transmettre à 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 campagne et par combinaison de campagne et genre, vous devez ajouter deux destinations d'événement : l'une avec uniquement campagne comme dimension, et l'autre avec campagne 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'[UpdateConfigurationSetEventDestination](#) opération dans la destination Amazon SES API V2 pour créer et mettre à jour des destinations d'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 de votre 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'UpdateConfigurationSetEventDestinationAPI 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 Gestion des identités et des accès AWS](#) (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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Action": [
        "firehose:PutRecordBatch"
      ],
      "Resource": [
        "arn:aws:firehose:us-east-1:111122223333:deliverystream/delivery-stream-name"
      ]
    }
  ]
}
```

Dans l'exemple précédent, apportez les modifications suivantes :

- *delivery-region* Remplacez-le 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.

JSON

```
{
  "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 :

- *delivery-region* Remplacez-le par la AWS région dans laquelle vous avez créé le flux de diffusion Firehose.
- Remplacez *111122223333* par votre ID de compte AWS .
- *configuration-set-name* Remplacez-le 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 les événements d'envoi d'e-mails que vous définissez lors de la création d'une destination d'événement 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 dans [Surveillance 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 dans [Création d'une destination d'événement](#).

Vous pouvez également utiliser l'[UpdateConfigurationSetEventDestination](#) opération 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 précédentes [Création 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 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'[UpdateConfigurationSetEventDestination](#) opération 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 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'[UpdateConfigurationSetEventDestination](#) opération 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 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 :

JSON

```
{
  "Version": "2012-10-17",
  "Id": "notification-policy",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ses.amazonaws.com"
      },
      "Action": "sns:Publish",
      "Resource": "arn:aws:sns:us-east-1:111122223333: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 :

- *topic_region* Remplacez-le par la AWS région dans laquelle vous avez créé le sujet SNS.
- Remplacez *111122223333* par votre identifiant de AWS compte.
- *topic_name* Remplacez-le par le nom de votre rubrique SNS.
- *configuration-set-name* Remplacez-le par le nom de votre ensemble 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

Interface d'envoi d'e-mails	Méthodes de publication d'événements
<code>SendCustomVerificationEmail</code>	Paramètres d'API
<code>SendRawEmail</code>	Paramètres d'API, en-têtes d'e-mail propres à Amazon SES ou en-têtes MIME personnalisés
	 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](#) avec la publication d'événements, vous devez spécifier le jeu de configuration et les balises 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-mail réussira toujours, mais les statistiques de l'événement ne seront pas transmises à 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.

- [Extraction des données d'événements Amazon SES depuis CloudWatch](#)
- [Récupération des données d'événements Amazon SES depuis Firehose](#)
- [Interprétation des données d'événement Amazon SES à partir d'Amazon SNS](#)

Extraction des données d'événements Amazon SES depuis CloudWatch

Amazon SES peut publier des statistiques relatives à vos événements d'envoi d'e-mails à Amazon CloudWatch. Lorsque vous publiez des données d'événements sur CloudWatch, il fournit ces

mesures sous la forme d'un ensemble ordonné de données de séries 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 CloudWatch alarme pour qu'elle se déclenche lorsque la métrique dépasse une certaine valeur.

Amazon SES peut publier ces événements à deux niveaux de granularité pour CloudWatch :

- Dans votre ensemble Compte AWS — Ces indicateurs grossiers, qui correspondent aux indicateurs que vous surveillez à l'aide de la console Amazon SES et de l'GetSendStatisticsAPI, sont des totaux pour l'ensemble Compte AWS de votre entreprise. Amazon SES publie ces statistiques CloudWatch automatiquement.
- 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 sur CloudWatch, vous devez [configurer la publication d'événements](#) avec une destination d' CloudWatch événement et [spécifier un ensemble de configuration](#) 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 statistiques d'envoi d'e-mails Amazon SES suivantes 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 ne sont inclus que lorsque SES n'essaie plus de

livrer l'e-mail. En général, ces rebonds souples indiquent un échec de livraison, bien que dans certains cas, un rebond souple puisse être renvoyé même lorsque le courrier parvient avec succès dans la boîte de réception du destinataire. Cela se produit généralement lorsque le destinataire envoie une réponse out-of-office automatique. Pour en savoir plus sur les soft bounces, consultez cet article de [AWS Re:Post](#).)

- 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.

Dimensions disponibles

CloudWatch utilise les noms de dimension que vous spécifiez lorsque vous ajoutez une destination d' CloudWatch événement à un ensemble de configuration dans Amazon SES. Pour de plus amples informations, veuillez consulter [Configurer une destination d' CloudWatch événement pour la publication d'événements](#).

Afficher les métriques Amazon SES dans la CloudWatch console

La procédure suivante explique comment consulter les métriques de publication de vos événements Amazon SES à l'aide de la CloudWatch console.

Pour afficher les métriques à l'aide de la CloudWatch console

1. Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/cloudwatch/>.
2. Si nécessaire, changez la région. Dans la barre de navigation, sélectionnez la région dans laquelle se trouvent vos AWS ressources. Pour plus d'informations, 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 CloudWatch les métriques Amazon](#).

Pour consulter les statistiques à l'aide du 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

- [Top-level Objet JSON](#)

- [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](#)

Top-level Objet JSON

L'objet JSON de niveau supérieur d'un registre d'événement d'envoi d'e-mail contient les champs suivants.

Nom de champ	Description
<code>eventType</code>	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 <code>notificationType</code> .
<code>mail</code>	Objet JSON qui contient des informations sur l'e-mail qui a généré l'événement.
<code>bounce</code>	Ce champ est présent uniquement si <code>eventType</code> a la valeur Bounce. Il contient des informations sur le retour à l'expéditeur.

Nom de champ	Description
complaint	Ce champ est présent uniquement si <code>eventType</code> a la valeur <code>Complaint</code> . Il contient des informations sur la réclamation.
delivery	Ce champ est présent uniquement si <code>eventType</code> a la valeur <code>Delivery</code> . Il contient des informations sur la remise.
send	Ce champ est présent uniquement si <code>eventType</code> a la valeur <code>Send</code> .
reject	Ce champ est présent uniquement si <code>eventType</code> a la valeur <code>Reject</code> . Il contient des informations sur le rejet.
open	Ce champ est présent uniquement si <code>eventType</code> a la valeur <code>Open</code> . Il contient des informations sur l'événement ouvert.
click	Ce champ est présent uniquement si <code>eventType</code> a la valeur <code>Click</code> . Il contient des informations sur l'événement de clic.
failure	Ce champ est présent uniquement si <code>eventType</code> a la valeur <code>Rendering Failure</code> . Il contient des informations sur l'événement d'échec d'affichage.
deliveryDelay	Ce champ est présent uniquement si <code>eventType</code> a la valeur <code>DeliveryDelay</code> . Il contient des informations sur la livraison différée d'un e-mail.

Nom de champ	Description
<code>subscription</code>	Ce champ est présent uniquement si <code>eventType</code> a la valeur <code>Subscription</code> . 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
<code>timestamp</code>	Date et heure, au format ISO8601 (YYYY-MM-DDThh:mm:ss.sZ), auxquelles le message a été envoyé.
<code>messageId</code>	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 <code>headers</code> et <code>commonHeaders</code> de l'objet <code>mail</code>.
<code>source</code>	Adresse e-mail à partir de laquelle le message a été envoyé (adresse MAIL FROM de l'enveloppe).
<code>sourceArn</code>	ARN (Amazon Resource Name) de l'identité qui a été utilisée pour envoyer l'e-mail. Dans

Nom de champ	Description
	le cas d'une autorisation d'envoi, <code>sourceArn</code> 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 .
<code>sendingAccountId</code>	L' AWS identifiant du compte utilisé pour envoyer l'e-mail. Dans le cas de l'autorisation d'envoi, <code>sendingAccountId</code> correspond à l'ID de compte de l'expéditeur délégué.
<code>destination</code>	Liste des adresses e-mail destinataires de l'e-mail original.
<code>headersTruncated</code>	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 <code>true</code> et <code>false</code> .
<code>headers</code>	Liste des en-têtes d'origine de l'e-mail. Chaque en-tête de la liste a un champ <code>name</code> et un champ <code>value</code>.  Note Tout ID de message du champ <code>headers</code> 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 <code>messageId</code> de l'objet <code>mail</code>.

Nom de champ	Description
<code>commonHeaders</code>	Mappage des en-têtes originaux de l'e-mail communément utilisés.  Note Tout ID de message contenu dans le champ <code>commonHeaders</code> correspond à l'ID de message qu'Amazon SES a par la suite affecté au message dans le champ <code>messageId</code> de l'objet <code>mail</code>.
<code>tags</code>	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
<code>bounceType</code>	Type de retour à l'expéditeur, tel que déterminé par Amazon SES.
<code>bounceSubType</code>	Sous-type de retour à l'expéditeur, tel que déterminé par Amazon SES.
<code>bouncedRecipients</code>	Liste qui contient les informations sur les destinataires de l'e-mail d'origine ayant fait l'objet d'un retour à l'expéditeur.
<code>timestamp</code>	Date et heure, au format ISO8601 (YYYY-MM-DDThh:mm:ss.sZ), auxquelles le fournisseur de services Internet a envoyé la notification de rebond.

Nom de champ	Description
<code>feedbackId</code>	ID unique du retour à l'expéditeur.
<code>reportingMTA</code>	Valeur du champ <code>Reporting-MTA</code> 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
<code>emailAddress</code>	Adresse e-mail du destinataire. Si un DSN est disponible, l'adresse correspond à la valeur du champ <code>Final-Recipient</code> 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
<code>action</code>	Valeur du champ <code>Action</code> du DSN. Cette valeur indique l'action effectuée par la MTA de suivi

Nom de champ	Description
	comme résultat de sa tentative de remettre le message à ce destinataire.
<code>status</code>	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.
<code>diagnosticCode</code>	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 événement 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`.

<code>bounceType</code>	rebondir SubType	Description
<code>Undetermined</code>	<code>Undetermined</code>	Amazon SES n'a pas pu déterminer de motif de retour à l'expéditeur.
<code>Permanent</code>	<code>General</code>	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.

bounceType	rebondir SubType	Description
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'expéditeur, 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 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.
Permanent	EmailValidationSuppressed	Amazon SES a supprimé l'envoi à cette adresse car celle-ci n'atteignait pas le seuil de vos paramètres de validation des e-mails .
Permanent	OnTenantSuppressionList	Amazon SES a supprimé l'envoi à cette adresse car celle-ci figure sur la liste de suppression au niveau du locataire . 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	rebondir SubType	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	CustomTimeoutExceeded	Amazon SES n'a pas réussi à envoyer l'e-mail dans le délai spécifié par l'expéditeur de l'e-mail. (Le message de rebond indiquera la raison de tout échec éventuel de tentative de livraison dans le cadre du TTL défini.)
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
<code>complainedRecipients</code>	Liste contenant des informations sur les destinataires qui ont soumis la réclamation.

Nom de champ	Description
<code>timestamp</code>	Date et heure, au format ISO8601 (YYYY-MM-DDThh:mm:ss.sZ), auxquelles le fournisseur de services Internet a envoyé la notification de plainte.
<code>feedbackId</code>	ID unique de la réclamation.
<code>complaintSubType</code>	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
<code>userAgent</code>	Valeur du champ User-Agent du rapport de commentaires. Cette valeur indique le nom et la version du système ayant généré le rapport.
<code>complaintFeedbackType</code>	Valeur du champ Feedback-Type du rapport de commentaires reçu de l'ISP. La valeur contient le type de commentaires.
<code>arrivalDate</code>	La valeur du Received-Date champ Arrival-Date ou du rapport de feedback 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
<code>emailAddress</code>	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 \(Internet Assigned Numbers\)](https://iana.org/domains/example/) :

Nom de champ	Description
<code>abuse</code>	Indique un e-mail indésirable ou un autre type d'e-mail malveillant.
<code>auth-failure</code>	Rapport d'échec d'authentification d'e-mail.
<code>fraud</code>	Indique certains types de fraude ou d'activité d'hameçonnage.
<code>not-spam</code>	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.
<code>other</code>	Indique tout autre commentaire ne pouvant être classé dans les autres types enregistrés.

Nom de champ	Description
<code>virus</code>	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
<code>timestamp</code>	Date et heure auxquelles Amazon SES a envoyé l'e-mail au serveur de messagerie du destinataire, au format ISO8601 () YYYY-MM-DDThh:mm:ss.sZ.
<code>processingTimeMillis</code>	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.
<code>recipients</code>	Liste des destinataires auxquels l'événement de remise s'applique.
<code>smtpResponse</code>	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.
<code>reportingMTA</code>	Nom d'hôte du serveur de messagerie Amazon SES ayant envoyé l'e-mail.
<code>remoteMtaIp</code>	Adresse IP de la MTA à laquelle Amazon SES a remis 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 <code>BadContent</code> , 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 ouvert s'est produit au format ISO8601 (<code>() YYYY-MM-DDThh:mm:ss.sZ</code>).
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
<code>ipAddress</code>	Adresse IP du destinataire.
<code>timestamp</code>	Date et heure auxquelles l'événement de clic s'est produit au format ISO8601 () YYYY-MM-DDThh:mm:ss.sZ.
<code>userAgent</code>	Agent utilisateur du client que le destinataire a utilisé pour cliquer sur un lien dans l'e-mail.
<code>link</code>	URL du lien sur lequel le destinataire a cliqué.
<code>linkTags</code>	Liste des balises ajoutées au lien à l'aide de l'attribut <code>ses:tags</code> . 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 Statistiques d'envoi d'e-mails Amazon SES FAQs .

Objet Rendering Failure

L'objet JSON qui contient les informations sur un événement `Rendering Failure` comporte les champs suivants.

Nom de champ	Description
<code>templateName</code>	Nom du modèle utilisé pour envoyer l'e-mail.
<code>errorMessage</code>	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
<code>delayType</code>	Type de retard. Les valeurs possibles sont : • <code>InternalFailure</code>— Un problème interne à Amazon SES a retardé le message. • <code>General</code> – Une défaillance générique s'est produite au cours de la conversation SMTP. • <code>MailboxFull</code>— La boîte aux lettres du destinataire est pleine et ne peut pas recevoir de messages supplémentaires. • <code>SpamDetected</code>— Le serveur de messagerie du destinataire a détecté un grand nombre d'e-mails non sollicités provenant de votre compte. • <code>RecipientServerError</code>— Un problème temporaire avec le serveur de messagerie du destinataire empêche la livraison du message. • <code>IPFailure</code> – L'adresse IP qui envoie le message est bloquée ou réduite par le fournisseur de messagerie du destinataire. • <code>TransientCommunicationFailure</code>— Un échec de communication temporaire s'est produit lors de la conversation SMTP avec le fournisseur de messagerie du destinataire. • <code>BYOIPHostNameLookupUnavailable</code>— 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

Nom de champ	Description
	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.
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
<code>contactList</code>	Nom de la liste sur laquelle figure le contact.
<code>timestamp</code>	Date et heure, au format ISO8601 (YYYY-MM-DDThh:mm:ss.sZ), auxquelles le fournisseur de services Internet a envoyé la notification d'abonnement.
<code>source</code>	Adresse e-mail à partir de laquelle le message a été envoyé (adresse MAIL FROM de l'enveloppe).
<code>newTopicPreferences</code>	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).
<code>oldTopicPreferences</code>	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).

New/old préférences de sujet

Les objets `newTopicPreferences` et `oldTopicPreferences` contiennent les valeurs suivantes.

Nom de champ	Description
<code>unsubscribeAll</code>	Indique si le contact s'est désabonné de toutes les rubriques de la liste de contacts.

Nom de champ	Description
<code>topicSubscriptionStatus</code>	Spécifie le statut d'abonnement du sujet dans le <code>topicName</code> champ indiquant s'il est actuellement abonné pour recevoir des notifications de SES pour le type d'événement spécifié. Les valeurs possibles sont <code>OptIn(abonné)</code> ou <code>OptOut(désabonné)</code> dans le <code>subscriptionStatus</code> champ.
<code>topicDefaultSubscriptionStatus</code>	Spécifie le statut d'abonnement par défaut du sujet dans le <code>topicName</code> champ déterminant si les nouveaux sujets ajoutés à la destination de l'événement seront abonnés ou désabonnés par défaut. Les valeurs possibles sont <code>OptIn(abonné par défaut)</code> ou <code>OptOut(désabonné par défaut)</code> dans le <code>subscriptionStatus</code> 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'Complaintévénement 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",
  "remoteMtaIp": "123.456.789.012",
  "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'Openévénement publié par Amazon SES sur Firehose.

```
{
  "eventType": "Open",
  "mail": {
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-0000000",
      "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'Clickévénement 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-0000000",
      "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-0000000",
    "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-0000000",
    "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-f515137b1497-0000000",
    "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 :

- [Top-level Objet JSON](#)
- [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](#)

Top-level Objet JSON

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 . 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.

Nom de champ	Description
<code>click</code>	Ce champ est présent uniquement si <code>eventType</code> a la valeur <code>Click</code> . Il contient des informations sur l'événement de clic.
<code>failure</code>	Ce champ est présent uniquement si <code>eventType</code> a la valeur <code>Rendering Failure</code> . Il contient des informations sur l'événement d'échec d'affichage.
<code>deliveryDelay</code>	Ce champ est présent uniquement si <code>eventType</code> a la valeur <code>DeliveryDelay</code> . Il contient des informations sur la livraison différée d'un e-mail.
<code>subscription</code>	Ce champ est présent uniquement si <code>eventType</code> a la valeur <code>Subscription</code> . 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
<code>timestamp</code>	Date et heure, au format ISO8601 (YYYY-MM-DDThh:mm:ss.sZ), auxquelles le message a été envoyé.
<code>messageId</code>	ID unique attribué par Amazon SES au message. Amazon SES vous a renvoyé cette valeur lorsque vous avez envoyé le message.

Nom de champ	Description
	 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	L' AWS identifiant du compte qui a été 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
<code>headers</code>	Liste des en-têtes d'origine de l'e-mail. Chaque en-tête de la liste a un champ <code>name</code> et un champ <code>value</code>.  Note Tout ID de message du champ <code>headers</code> 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 <code>messageId</code> de l'objet <code>mail</code>.
<code>commonHeaders</code>	Mappage des en-têtes originaux de l'e-mail communément utilisés.  Note Tout ID de message contenu dans le champ <code>commonHeaders</code> correspond à l'ID de message qu'Amazon SES a par la suite affecté au message dans le champ <code>messageId</code> de l'objet <code>mail</code>.
<code>tags</code>	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 (YYYY-MM-DDThh:mm:ss.sZ), auxquelles le fournisseur de services Internet a envoyé la notification de rebond.
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
<code>emailAddress</code>	Adresse e-mail du destinataire. Si un DSN est disponible, l'adresse correspond à la valeur du champ <code>Final-Recipient</code> 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
<code>action</code>	Valeur du champ <code>Action</code> 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.
<code>status</code>	Valeur du champ <code>Status</code> du DSN. Il s'agit du code de statut indépendant du transport par destinataire qui indique le statut de remise du message.
<code>diagnosticCode</code>	Code de statut émis par la MTA de suivi. Il s'agit de la valeur du champ <code>Diagnostic-Code</code> du DSN. Ce champ peut être absent du DSN (et donc également absent du JSON).

Types de retour à l'expéditeur

Chaque événement 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	rebondir SubType	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'expéditeur, 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 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.
Permanent	EmailValidationSuppressed	Amazon SES a supprimé l'envoi à cette adresse car celle-ci n'atteignait pas le seuil de vos paramètres de validation des e-mails .

bounceType	rebondir SubType	Description
Permanent	OnTenantSuppressionList	Amazon SES a supprimé l'envoi à cette adresse car celle-ci figure sur la liste de suppression au niveau du locataire . 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.
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	CustomTimeoutExceeded	Amazon SES n'a pas réussi à envoyer l'e-mail dans le délai spécifié par l'expéditeur de l'e-mail. (Le message de rebond indiquera la raison de tout échec éventuel de tentative de livraison dans le cadre du TTL défini.)
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
<code>complainedRecipients</code>	Liste contenant des informations sur les destinataires qui ont soumis la réclamation.
<code>timestamp</code>	Date et heure, au format ISO8601 (YYYY-MM-DDThh:mm:ss.sZ), auxquelles le fournisseur de services Internet a envoyé la notification de plainte.
<code>feedbackId</code>	ID unique de la réclamation.
<code>complaintSubType</code>	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
<code>userAgent</code>	Valeur du champ <code>User-Agent</code> du rapport de commentaires. Cette valeur indique le nom et la version du système ayant généré le rapport.
<code>complaintFeedbackType</code>	Valeur du champ <code>Feedback-Type</code> du rapport de commentaires reçu de l'ISP. La valeur contient le type de commentaires.
<code>arrivalDate</code>	La valeur du <code>Received-Date</code> champ <code>Arrival-Date</code> ou du rapport de feedback 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
<code>emailAddress</code>	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 \(Internet Assigned Numbers\)](https://www.iana.org/domains/reserved) :

Nom de champ	Description
<code>abuse</code>	Indique un e-mail indésirable ou un autre type d'e-mail malveillant.
<code>auth-failure</code>	Rapport d'échec d'authentification d'e-mail.
<code>fraud</code>	Indique certains types de fraude ou d'activité d'hameçonnage.
<code>not-spam</code>	Indique que l'entité qui fournit le rapport ne considère pas le message en tant que courrier indésirable. Cette option permet de corriger un

Nom de champ	Description
	message qui a été mal balisé ou classé à tort comme courrier indésirable.
<code>other</code>	Indique tout autre commentaire ne pouvant être classé dans les autres types enregistrés.
<code>virus</code>	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](#). La valeur peut également être `OnTenantSuppressionList` si l'adresse figurait sur la liste de [suppression au niveau du locataire](#).

Objet Delivery

L'objet JSON qui contient les informations sur un événement `Delivery` comporte les champs suivants.

Nom de champ	Description
<code>timestamp</code>	Date et heure auxquelles Amazon SES a envoyé l'e-mail au serveur de messagerie du destinataire, au format ISO8601 () YYYY-MM-DDThh:mm:ss.sZ.
<code>processingTimeMillis</code>	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.

Nom de champ	Description
<code>recipients</code>	Liste des destinataires auxquels l'événement de remise s'applique.
<code>smtpResponse</code>	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.
<code>reportingMTA</code>	Nom d'hôte du serveur de messagerie Amazon SES ayant envoyé l'e-mail.
<code>remoteMtaIp</code>	Adresse IP de la MTA à laquelle Amazon SES a remis 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
<code>reason</code>	Raison du rejet de l'e-mail. La seule valeur possible est <code>BadContent</code> , 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
<code>ipAddress</code>	Adresse IP du destinataire.
<code>timestamp</code>	Date et heure auxquelles l'événement ouvert s'est produit au format ISO8601 () YYYY-MM-DDThh:mm:ss.sZ.
<code>userAgent</code>	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
<code>ipAddress</code>	Adresse IP du destinataire.
<code>timestamp</code>	Date et heure auxquelles l'événement de clic s'est produit au format ISO8601 () YYYY-MM-DDThh:mm:ss.sZ.
<code>userAgent</code>	Agent utilisateur du client que le destinataire a utilisé pour cliquer sur un lien dans l'e-mail.
<code>link</code>	URL du lien sur lequel le destinataire a cliqué.
<code>linkTags</code>	Liste des balises ajoutées au lien à l'aide de l'attribut <code>ses:tags</code> . 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 Statistiques d'envoi d'e-mails Amazon SES FAQs .

Objet Rendering Failure

L'objet JSON qui contient les informations sur un événement `Rendering Failure` comporte les champs suivants.

Nom de champ	Description
<code>templateName</code>	Nom du modèle utilisé pour envoyer l'e-mail.
<code>errorMessage</code>	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
<code>delayType</code>	Type de retard. Les valeurs possibles sont : • <code>InternalFailure</code>— Un problème interne à Amazon SES a retardé le message. • <code>General</code> – Une défaillance générique s'est produite au cours de la conversation SMTP. • <code>MailboxFull</code>— La boîte aux lettres du destinataire est pleine et ne peut pas recevoir de messages supplémentaires. • <code>SpamDetected</code>— Le serveur de messagerie du destinataire a détecté un grand nombre d'e-mails non sollicités provenant de votre compte. • <code>RecipientServerError</code>— Un problème temporaire avec le serveur de messagerie du destinataire empêche la livraison du message.

Nom de champ	Description
	• 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. • BYOIPHostNameLookupUnavailable— 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. • 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
<code>emailAddress</code>	Adresse électronique ayant entraîné un retard dans la livraison du message.
<code>status</code>	Code d'état SMTP associé au délai de livraison.
<code>diagnosticCode</code>	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
<code>contactList</code>	Nom de la liste sur laquelle figure le contact.
<code>timestamp</code>	Date et heure, au format ISO8601 (YYYY-MM-DDThh:mm:ss.sZ), auxquelles le fournisseur de services Internet a envoyé la notification d'abonnement.
<code>source</code>	Adresse e-mail à partir de laquelle le message a été envoyé (adresse MAIL FROM de l'enveloppe).
<code>newTopicPreferences</code>	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).
<code>oldTopicPreferences</code>	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).

New/old préférences de sujet

Les objets `newTopicPreferences` et `oldTopicPreferences` contiennent les valeurs suivantes.

Nom de champ	Description
<code>unsubscribeAll</code>	Indique si le contact s'est désabonné de toutes les rubriques de la liste de contacts.
<code>topicSubscriptionStatus</code>	Spécifie le statut d'abonnement du sujet dans le <code>topicName</code> champ indiquant s'il est actuellement abonné pour recevoir des notifications de SES pour le type d'événement spécifié. Les valeurs possibles sont <code>OptIn</code> (abonné) ou <code>OptOut</code> (désabonné) dans le <code>subscriptionStatus</code> champ.
<code>topicDefaultSubscriptionStatus</code>	Spécifie le statut d'abonnement par défaut du sujet dans le <code>topicName</code> champ déterminant si les nouveaux sujets ajoutés à la destination de l'événement seront abonnés ou désabonnés par défaut. Les valeurs possibles sont <code>OptIn</code> (abonné par défaut) ou <code>OptOut</code> (désabonné par défaut) dans le <code>subscriptionStatus</code> 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 :

- [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](#)
- [Enregistrement d'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

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",
"remoteMtaIp": "123.456.789.012",
"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-0000000",
    "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-0000000",
    "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 Open 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-0000000",
    "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

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-0000000",
    "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": "EXAMPLEEe4bccb684-777bc8de-afa7-4970-92b0-f515137b1497-0000000",
    "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 en utilisant CloudWatch](#)
- [Métriques SNDS pour les applications dédiées IPs](#)
- [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 console Amazon SES AWS Management Console et ouvrez-la 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 [Processus de révision d'Amazon SES Sending FAQs](#).
 - 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 [Processus de révision d'Amazon SES Sending FAQs](#).
 - **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 [Processus de révision d'Amazon SES Sending FAQs](#).
- 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 [Processus de révision d'Amazon SES Sending FAQs](#).

- 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 a déjà été suspendue, connectez-vous au AWS Management Console et rendez-vous sur [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 modifications susceptibles de résoudre le problème, 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 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 reconsidérons cette décision. Pour de plus amples informations, veuillez consulter [Processus de révision d'Amazon SES Sending FAQs](#).

Lorsque vous mettez en œuvre des 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. 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 a déjà été suspendue, connectez-vous à la AWS console 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 modifications susceptibles de résoudre le problème, 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 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 reconsidérons cette décision. Pour de plus amples informations, veuillez consulter [Processus de révision d'Amazon SES Sending FAQs](#).

Lorsque vous avez mis en œuvre des modifications susceptibles de résoudre le problème, connectez-vous à la AWS console 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 modifications susceptibles de résoudre le problème, 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, 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 reconsidérons cette décision. Pour de plus amples informations, veuillez consulter [Processus de révision d'Amazon SES Sending FAQs](#).

Lorsque vous avez mis en œuvre des modifications susceptibles de résoudre le problème, connectez-vous à la AWS console 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 modifications susceptibles de résoudre le problème, 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, 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 reconsidérons cette décision. Pour de plus amples informations, veuillez consulter [Processus de révision d'Amazon SES Sending FAQs](#).

Lorsque vous avez mis en œuvre des modifications susceptibles de résoudre le problème, connectez-vous à la AWS console 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 modifications susceptibles de résoudre le problème, connectez-vous à la AWS console et rendez-vous 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 reconsidérons cette décision. Pour de plus amples informations, veuillez consulter [Processus de révision d'Amazon SES Sending FAQs](#).

Lorsque vous avez mis en œuvre des modifications susceptibles de résoudre le problème, connectez-vous à la AWS console 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 domaines bloquée de 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 modifications susceptibles de résoudre le problème, 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, 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 reconsidérons cette décision. Pour de plus amples informations, veuillez consulter [Processus de révision d'Amazon SES Sending FAQs](#).

Lorsque vous avez mis en œuvre des modifications susceptibles de résoudre le problème, connectez-vous à la AWS console 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 domaines bloquée de 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

Lorsque vous avez mis en œuvre des modifications susceptibles de résoudre le problème, connectez-vous à la AWS console 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 [Processus de révision d'Amazon SES Sending FAQs](#) 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 lettres 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 modifications susceptibles de résoudre le problème, 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, 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 reconsidérons cette décision. Pour de plus amples informations, veuillez consulter [Processus de révision d'Amazon SES Sending FAQs](#).

Lorsque vous avez mis en œuvre des modifications susceptibles de résoudre le problème, connectez-vous à la AWS console 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 modifications susceptibles de résoudre le problème, 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, 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 reconsidérons cette décision. Pour de plus amples informations, veuillez consulter [Processus de révision d'Amazon SES Sending FAQs](#).

Lorsque vous avez mis en œuvre des modifications susceptibles de résoudre le problème, connectez-vous à la AWS console 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 au vôtre Compte AWS, c'est pourquoi nous avons pris des mesures pour éviter des 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. Après avoir mis en œuvre 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. 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 surveillées 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 modifications susceptibles de résoudre le problème, 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, 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 reconsidérons cette décision. Pour de plus amples informations, veuillez consulter [Processus de révision d'Amazon SES Sending FAQs](#).

Lorsque vous avez mis en œuvre des modifications susceptibles de résoudre le problème, connectez-vous à la AWS console 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

Lorsque vous avez mis en œuvre des modifications susceptibles de résoudre le problème, connectez-vous à la AWS console 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 [Processus de révision d'Amazon SES Sending FAQs](#) 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

Lorsque vous avez mis en œuvre des modifications susceptibles de résoudre le problème, connectez-vous à la AWS console 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 [Processus de révision d'Amazon SES Sending FAQs](#) 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 Support Center, connectez-vous au, AWS Management Console puis choisissez Support Center. 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 en utilisant CloudWatch

Amazon SES publie automatiquement une série de statistiques 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 CloudWatch partie des procédures de cette section vise simplement à présenter les principales étapes de configuration d'une CloudWatch alarme afin de surveiller la réputation

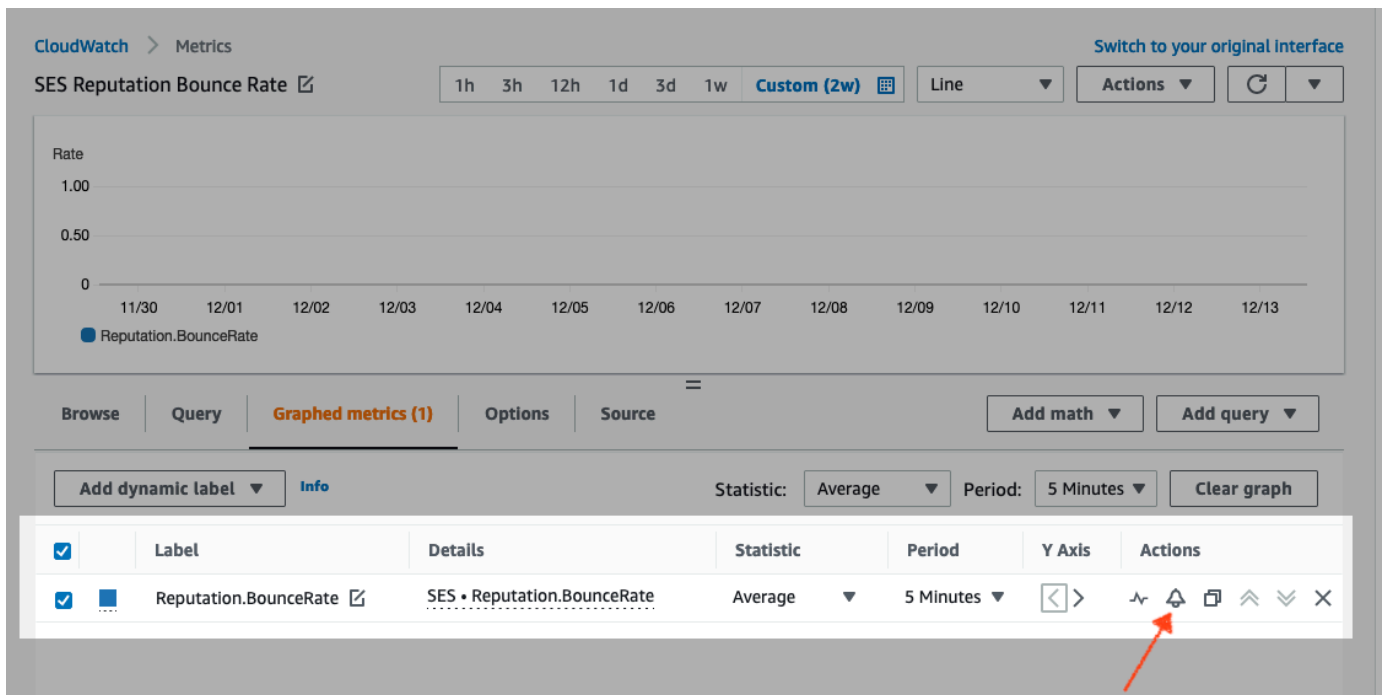
de votre expéditeur SES. Ils n'explorent pas les configurations avancées concernant les paramètres optionnels des CloudWatch alarmes. Pour obtenir des informations complètes sur la configuration des CloudWatch alarmes, consultez la section [Utilisation des CloudWatch alarmes Amazon](#) dans le guide de CloudWatch l'utilisateur Amazon.

Conditions préalables

- 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 CloudWatch alarme afin de surveiller la réputation des expéditeurs

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 sur le côté gauche de l'écran, choisissez Reputation Dashboard (Métriques de réputation).
3. Sur la page Mesures de réputation sous l'Account-levelonglet, dans le volet Taux de rebond ou Taux de plaintes, choisissez Afficher dans CloudWatch. Cela ouvrira la CloudWatch console avec la métrique que vous avez choisie.
4. Dans l'onglet Mesures graphiques, sur la ligne de la métrique que vous avez choisie, pour cet exemple Reputation.BounceRate, cliquez sur l'icône en forme de sonnette d'alarme dans la colonne Actions (voir image ci-dessous). Cela ouvrira la page Spécifier la métrique et les conditions.



5. Faites défiler jusqu'au panneau Conditions et choisissez Static (Statique) dans le champ Threshold type (Type de seuil).
 - a. Dans le Whenever **metric** is... champ, choisissez Greater/Equal.
 - b. Dans le bassin... champ, spécifiez la valeur qui doit provoquer CloudWatch le déclenchement d'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 pour vous envoyer une notification lorsque le taux de rebond de 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 pour vous envoyer une notification lorsque le taux de plaintes 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 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 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 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 applications dédiées IPs

Vous pouvez consulter les données SNDS (Smart Network Data Services) pour les adresses IP dédiées louées dans chaque Région AWS endroit où vous utilisez Amazon SES. Ces données SNDS sont disponibles via la CloudWatch console Amazon.

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 à ceux qui louent des véhicules dédiés IPs. 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 CloudWatch console Amazon 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).

(Des instructions sont données pour la nouvelle interface de CloudWatch console.)

3. Dans l'onglet Parcourir du conteneur Metrics, sélectionnez votre Région AWS, puis choisissez SES.
4. Choisissez IP Metrics qui vous montrera l'ensemble de vos données dédiées IPs suivies par le SNDS.

(Remarque : si aucune adresse IP dédiée n'est associée à votre compte dans la région sélectionnée, les mesures IP n'apparaîtront pas dans la CloudWatch console.)

5. Consultez l'ensemble de vos données dédiées IPs suivies par le SNDS dans cette liste, ou sélectionnez une adresse IP individuelle pour n'afficher que ses indicateurs.

Les métriques suivantes sont fournies pour chaque adresse IP dédiée et sont définies par Outlook. Pour plus d'informations, consultez la section SNDS [FAQs](#) d'Outlook.

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 le SNDS pour l'adresse IP spécifique pendant 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 - Le nombre de commandes DATA perçues par le SNDS pour l'adresse IP spécifique pendant 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 - Le nombre de destinataires des messages perçus par le SNDS pour l'adresse IP spécifique pendant la période d'activité.
- SNDS. SpamRate - Affiche les résultats agrégés du filtrage anti-spam appliqué à tous les messages envoyés par l'adresse IP au cours de la période d'activité donnée.
 - Une SpamRate valeur de 0 signifie que l'adresse IP contient moins de 10 % de spam.
 - Une valeur SpamRate de 0,5 signifie qu'entre 10 % et 90 % de spam sont générés à partir de l'adresse IP.
 - Une valeur SpamRate de 1 signifie que 90 % ou plus de spam est généré à partir de l'adresse IP.
- SNDS. ComplaintRate - Il s'agit de la fraction du temps pendant laquelle un message reçu de l'adresse IP fait l'objet d'une plainte par un utilisateur d'Outlook pendant la période d'activité.
 - Une note ComplaintRate de 1 correspond à un taux de plaintes de 100 %.
 - Un A ComplaintRate de 0,05 signifierait un taux de plaintes de 5 %, par exemple.
 - Une ComplaintRate valeur de 0 signifie que le taux est inférieur à 0,1 %.
- SNDS. TrapHits - Affiche le nombre de messages envoyés pour « piéger des comptes ». 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 SNDS ? SpamRate et SNDS. ComplaintRate les métriques changent, et que dois-je faire si le taux passe à une valeur de 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 (ISPs) ainsi que vos numéros d'engagement pour vous assurer qu'il ne s'agit pas d'un problème mondial. S'il s'agit d'un problème global, vous pouvez rencontrer des problèmes liés à

plusieurs ISPs, 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 AWS Support mesures seront prises si mon SNDS. SpamRate passe d'une valeur de 0 (ou 0,5) à 1 ?

AWS n'a aucun contrôle sur le SNDS et n'a donc aucune influence sur le 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 suspendre temporairement l'envoi d'e-mails pour les messages envoyés à l'aide d'ensembles de configuration spécifiques, ou pour tous les messages envoyés depuis votre compte Amazon SES dans une AWS région spécifique.

En utilisant Amazon CloudWatch et Lambda, vous pouvez créer une solution qui interrompt automatiquement l'envoi de vos e-mails lorsque vos indicateurs de réputation (tels que le taux de rebond ou le taux de plaintes) dépassent certains seuils. 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 décrites dans cette section expliquent les étapes à suivre pour configurer Amazon SES, Amazon SNS CloudWatch, Amazon et AWS Lambda pour suspendre automatiquement l'envoi d'e-mails pour votre compte Amazon SES dans une seule AWS région. 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](#)

- [2e partie : Créer la fonction Lambda](#)
- [3e partie : Réactivation de l'envoi d'e-mails pour votre compte](#)
- [4e partie : Créer une rubrique Amazon SNS et s'abonner](#)
- [Partie 5 : Création d'une CloudWatch alarme](#)
- [6e partie : Test de la solution](#)

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
 - Amazon SESFull Access

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.

Ensuite, sélectionnez 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 AWS Lambda console 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 uniquement l'envoi d'e-mails dans la AWS région que vous avez sélectionnée à 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. Sélectionnez 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, vous ne souhaitez pas suspendre l'envoi pour votre compte tant que l' CloudWatch alarme 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 plus d'informations, consultez 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. *sending_region* Remplacez-le 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

CloudWatch Pour exécuter votre fonction Lambda lorsqu'une alarme est déclenchée, vous devez d'abord créer une rubrique Amazon SNS et y abonner la fonction Lambda.

Pour créer une rubrique Amazon SNS et y abonner la fonction Lambda

1. [Ouvrez la console Amazon SNS à l'adresse v3/home. https://console.aws.amazon.com/sns/](https://console.aws.amazon.com/sns/)
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”](#).

Partie 5 : Création d'une CloudWatch alarme

Cette section contient des procédures permettant de créer une alarme déclenchée lorsqu'une métrique atteint un certain seuil. CloudWatch 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 CloudWatch alarme

1. Ouvrez la CloudWatch console 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 :

- Réputation. BounceRate — Choisissez cette métrique si vous souhaitez suspendre l'envoi d'e-mails pour votre compte lorsque le taux de rebond total de votre compte dépasse un seuil que vous avez défini.
- Réputation. ComplaintRate — Choisissez cette métrique si vous souhaitez suspendre l'envoi d'e-mails pour votre compte lorsque le taux global de plaintes pour votre compte dépasse un seuil que vous définissez.

Choisissez Suivant.

7. Procédez comme suit :

- Sous Alarm Threshold (Seuil d'alarme), pour Name (Nom), saisissez un nom pour l'alarme.
- Sous Whenever : Réputation. BounceRate ou à chaque fois : réputation. ComplaintRate, spécifiez le seuil qui déclenche l'alarme.

Note

Votre compte est automatiquement examiné si votre taux de rebond dépasse 5 % ou si votre taux de plaintes dépasse 0,1 %. Lorsque vous spécifiez le taux de rebond ou de plaintes à l'origine du déclenchement de l' CloudWatch alarme, nous vous recommandons d'utiliser des valeurs inférieures à ces taux pour éviter que votre compte ne soit examiné.

- 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`

Remplacez *MyAlarm* la commande précédente par le nom de l'alarme que vous avez créée et remplacez-la *region* par la région dans laquelle vous souhaitez suspendre automatiquement l'envoi d'e-mails. [the section called “Partie 5 : Création d'une CloudWatch alarme”](#)

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 consulter ces changements d'état dans l'onglet Historique de l'alarme de la CloudWatch console ou en utilisant l'[DescribeAlarmHistory](#) opération.

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 indicateurs de réputation spécifiques aux e-mails envoyés à l'aide d'une configuration spécifique définie à Amazon CloudWatch. Vous pouvez ensuite utiliser ces métriques pour créer des CloudWatch alarmes spécifiques à ces ensembles de configuration. 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 une configuration spécifique définie dans une seule AWS région. 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](#)
- [2e partie : Création d'un rôle IAM](#)
- [3e partie : Création de la fonction Lambda](#)
- [4e partie : Réactivation de l'envoi d'e-mails pour l'ensemble de configurations](#)
- [5e partie : Créer une rubrique Amazon SNS](#)
- [Partie 6 : Création d'une CloudWatch alarme](#)
- [7e partie : Test de la solution](#)

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 Lambda BasicExecutionRole
 - Amazon SESFull Access (nous vous recommandons d'utiliser un rôle personnalisé adapté à vos besoins, qui inclut les autorisations d'appel [UpdateConfigurationSetSendingEnabled](#).)

 Tip

Pour accéder rapidement à ces stratégies, servez-vous de la zone de recherche située en haut de la liste des stratégies.

Choisissez 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 AWS Lambda console 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';

import {
    SES
}
from 'aws-sdk';

const ses = new SES();
const configSet = 'CONFIG_SET_NAME_HERE';

const params = {
    ConfigurationSetName: configSet,
    Enabled: false
};

export const handler = async (event) => {
    try {
        const data = await
ses.updateConfigurationSetSendingEnabled(params).promise();

        console.log('Configuration Set Update:', data);

        return {
            statusCode: 200,
            body: JSON.stringify({
                message: 'Successfully paused email sending for configuration
set.',
                data
            }),
        };
    }
    catch (err) {
```

```
        console.error('Error:', err.message);
        return {
            statusCode: 500,
            body: JSON.stringify({
                message: 'Failed to pause email sending for configuration set.',
                error: err.message
            }),
        };
    }
};
```

Remplacez *ConfigSet* le code précédent par le nom du jeu de configuration. Choisissez 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 suspendre l'envoi de l'ensemble de configuration tant que l' CloudWatch alarme 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 plus d'informations, consultez 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 configuration pour lequel vous souhaitez suspendre 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

CloudWatch Pour exécuter la fonction Lambda lorsqu'une alarme est déclenchée, vous devez d'abord créer une rubrique Amazon SNS et y abonner la fonction Lambda.

Pour créer la rubrique Amazon SNS

1. [Ouvrez la console Amazon SNS à l'adresse v3/home. https://console.aws.amazon.com/sns/](https://console.aws.amazon.com/sns/)
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).

Partie 6 : Création d'une CloudWatch alarme

Cette section contient des procédures permettant de créer une alarme déclenchée lorsqu'une métrique atteint un certain seuil. CloudWatch 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 CloudWatch alarme

1. Ouvrez la CloudWatch console 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 :
 - Réputation. BounceRate — Choisissez cette métrique si vous souhaitez suspendre l'envoi d'e-mails pour le jeu de configuration lorsque le taux de rebond total du jeu de configuration dépasse un seuil que vous définissez.
 - Réputation. ComplaintRate — Choisissez cette métrique si vous souhaitez suspendre l'envoi d'e-mails pour l'ensemble de configuration lorsque le taux de plaintes global pour l'ensemble de configuration dépasse un seuil que vous définissez.

Choisissez Suivant.

7. Procédez comme suit :
 - Sous Alarm Threshold (Seuil d'alarme), pour Name (Nom), saisissez un nom pour l'alarme.
 - Sous Whenever : Réputation. BounceRate ou à chaque fois : réputation. ComplaintRate, spécifiez le seuil à partir duquel l'alarme se déclenche.

 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 rebond ou de plaintes à l'origine du déclenchement de l' CloudWatch alarme, nous vous recommandons d'utiliser des valeurs bien inférieures à ces taux afin d'éviter que votre compte ne soit revu.

- 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'`SetAlarmState` opération de l' CloudWatch API 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"
```

Remplacez *MyAlarm* la commande précédente par le nom de l'alarme que vous avez créée dans [the section called “Partie 6 : Création d'une CloudWatch alarme”](#).

 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 consulter ces changements d'état dans l'onglet Historique de l'alarme de la CloudWatch console ou en utilisant l'[DescribeAlarmHistory](#) opération.

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 les événements que vous définissez lors de la création d'une destination d'événement 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](#)
- [Référence du schéma des événements SES](#)
- [Utilisation EventBridge avec des événements SES](#)
- [EventBridge Ressources supplémentaires](#)

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'événement 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 essaiera de transmettre 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 <code>List-Unsubscribe</code> dans l'en-tête de l'e-mail ou sur le <code>Unsubscribe</code> 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 dans [the 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](#)
- [Schéma d'état d'envoi d'e-mails SES](#)

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 dans [the 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.

Exemple 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 dans [the 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, voir [Spécifiez 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-0000000",
      "destination": ["recipient@example.com"],
      "headersTruncated": false,
      "tags": {
        "ses:configuration-set": ["ConfigSet"]
      }
    },
    "failure": {
      "errorMessage": "Attribute 'attributeName' is not present in the rendering data.",
      "templateName": "MyTemplate"
    }
  }
}
```

Exemple 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-0000000",
    "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 de lire 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 à l'aide de AWS SDKs

Les exemples de code suivants montrent comment utiliser Amazon SES avec un kit de développement AWS logiciel (SDK).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit 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 utilisant AWS Kits SDK](#)
- [Exemples de base pour l'utilisation d'Amazon SES AWS Kits SDK](#)
 - [Actions pour Amazon SES utilisant AWS Kits SDK](#)
 - [À utiliser CreateReceiptFilteravec un AWS Kit SDK](#)
 - [À utiliser CreateReceiptRuleavec un AWS Kit SDK](#)
 - [À utiliser CreateReceiptRuleSetavec un AWS Kit SDK](#)
 - [À utiliser CreateTemplateavec un AWS Kit SDK](#)
 - [À utiliser DeleteIdentityavec un AWS SDK ou CLI](#)
 - [À utiliser DeleteReceiptFilteravec un AWS Kit SDK](#)
 - [À utiliser DeleteReceiptRuleavec un AWS Kit SDK](#)
 - [À utiliser DeleteReceiptRuleSetavec un AWS Kit SDK](#)
 - [À utiliser DeleteTemplateavec un AWS Kit SDK](#)
 - [À utiliser DescribeReceiptRuleSetavec un AWS Kit SDK](#)
 - [À utiliser GetIdentityVerificationAttributesavec un AWS SDK ou CLI](#)
 - [À utiliser GetSendQuotaavec un AWS SDK ou CLI](#)
 - [Utilisation de GetSendStatistics avec une CLI](#)
 - [À utiliser GetTemplateavec un AWS Kit SDK](#)
 - [À utiliser ListIdentitiesavec un AWS SDK ou CLI](#)
 - [À utiliser ListReceiptFiltersavec un AWS Kit SDK](#)
 - [À utiliser ListTemplatesavec un AWS Kit SDK](#)
 - [À utiliser SendBulkTemplatedEmailavec un AWS Kit SDK](#)

- [À utiliser SendEmailavec un AWS SDK ou CLI](#)
- [À utiliser SendRawEmailavec un AWS SDK ou CLI](#)
- [À utiliser SendTemplatedEmailavec un AWS Kit SDK](#)
- [À utiliser UpdateTemplateavec un AWS Kit SDK](#)
- [À utiliser VerifyDomainIdentityavec un AWS SDK ou CLI](#)
- [À utiliser VerifyEmailIdentityavec un AWS SDK ou CLI](#)
- [Scénarios d'utilisation d'Amazon SES AWS Kits SDK](#)
 - [Créer une application de streaming Amazon Transcribe](#)
 - [Copiez les adresses e-mail et de domaine d'Amazon SES à partir d'un AWS Région vers une autre à l'aide d'un AWS Kit SDK](#)
 - [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 AWS Kit SDK](#)
 - [Détectez des objets dans des images avec Amazon Rekognition à l'aide d'un AWS Kit SDK](#)
 - [Détectez les personnes et les objets dans une vidéo avec Amazon Rekognition à l'aide d'un AWS Kit SDK](#)
 - [Générer des informations d'identification pour vous connecter à un point de terminaison d'un SMTP Amazon SES](#)
 - [Configuration des services d'envoi d'e-mails](#)
 - [Utiliser les fonctions Step Functions pour invoquer des fonctions Lambda](#)
 - [Vérifiez une identité e-mail et envoyez des messages à Amazon SES à l'aide d'un AWS Kit SDK](#)
- [Exemples de code pour l'API Amazon SES v2 à l'aide de AWS Kits SDK](#)
- [Exemples de base d'utilisation de l'API Amazon SES v2 AWS Kits SDK](#)
 - [Bonjour Amazon SES API v2](#)
 - [Actions pour l'API Amazon SES v2 à l'aide de AWS Kits SDK](#)
 - [À utiliser CreateContactavec un AWS Kit SDK](#)
 - [À utiliser CreateContactListavec un AWS Kit SDK](#)
 - [À utiliser CreateEmailIdentityavec un AWS Kit SDK](#)
 - [À utiliser CreateEmailTemplateavec un AWS Kit SDK](#)

- [À utiliser DeleteContactListavec un AWS Kit SDK](#)
- [À utiliser DeleteEmailIdentityavec un AWS Kit SDK](#)
- [À utiliser DeleteEmailTemplateavec un AWS Kit SDK](#)
- [À utiliser GetEmailIdentityavec un AWS Kit SDK](#)
- [À utiliser ListContactListsavec un AWS Kit SDK](#)
- [À utiliser ListContactsavec un AWS Kit SDK](#)
- [À utiliser SendBulkEmailavec un AWS Kit SDK](#)
- [À utiliser SendEmailavec un AWS Kit SDK](#)
- [Scénarios d'utilisation de l'API Amazon SES v2 AWS Kits SDK](#)
 - [Envoyer des e-mails avec des pièces jointes à l'aide de l'API Amazon SES v2](#)
 - [Un scénario complet de newsletter Amazon SES API v2 utilisant un AWS Kit SDK](#)

Exemples de code pour Amazon SES utilisant 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.

Les scénarios sont des exemples de code qui vous montrent comment accomplir des tâches spécifiques en appelant plusieurs fonctions au sein d'un même service ou combinés à d'autres Services AWS.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Amazon SES

- [Exemples de base pour l'utilisation d'Amazon SES AWS Kits SDK](#)
 - [Actions pour Amazon SES utilisant AWS Kits SDK](#)
 - [À utiliser CreateReceiptFilteravec un AWS Kit SDK](#)
 - [À utiliser CreateReceiptRuleavec un AWS Kit SDK](#)
 - [À utiliser CreateReceiptRuleSetavec un AWS Kit SDK](#)

- [À utiliser CreateTemplateavec un AWS Kit SDK](#)
- [À utiliser Deleteldentityavec un AWS SDK ou CLI](#)
- [À utiliser DeleteReceiptFilteravec un AWS Kit SDK](#)
- [À utiliser DeleteReceiptRuleavec un AWS Kit SDK](#)
- [À utiliser DeleteReceiptRuleSetavec un AWS Kit SDK](#)
- [À utiliser DeleteTemplateavec un AWS Kit SDK](#)
- [À utiliser DescribeReceiptRuleSetavec un AWS Kit SDK](#)
- [À utiliser GetldentityVerificationAttributesavec un AWS SDK ou CLI](#)
- [À utiliser GetSendQuotaavec un AWS SDK ou CLI](#)
- [Utilisation de GetSendStatistics avec une CLI](#)
- [À utiliser GetTemplateavec un AWS Kit SDK](#)
- [À utiliser ListIdentitiesavec un AWS SDK ou CLI](#)
- [À utiliser ListReceiptFiltersavec un AWS Kit SDK](#)
- [À utiliser ListTemplatesavec un AWS Kit SDK](#)
- [À utiliser SendBulkTemplatedEmailavec un AWS Kit SDK](#)
- [À utiliser SendEmailavec un AWS SDK ou CLI](#)
- [À utiliser SendRawEmailavec un AWS SDK ou CLI](#)
- [À utiliser SendTemplatedEmailavec un AWS Kit SDK](#)
- [À utiliser UpdateTemplateavec un AWS Kit SDK](#)
- [À utiliser VerifyDomainldentityavec un AWS SDK ou CLI](#)
- [À utiliser VerifyEmailldentityavec un AWS SDK ou CLI](#)
- [Scénarios d'utilisation d'Amazon SES AWS Kits SDK](#)
 - [Créer une application de streaming Amazon Transcribe](#)
 - [Copiez les adresses e-mail et de domaine d'Amazon SES à partir d'un AWS Région vers une autre à l'aide d'un AWS Kit SDK](#)
 - [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 AWS Kit SDK](#)
- [Détectez des objets dans des images avec Amazon Rekognition à l'aide d'un AWS Kit SDK](#)

- [Déterminez les personnes et les objets dans une vidéo avec Amazon Rekognition à l'aide d'un AWS Kit SDK](#)
- [Générer des informations d'identification pour vous connecter à un point de terminaison d'un SMTP Amazon SES](#)
- [Configuration des services d'envoi d'e-mails](#)
- [Utiliser les fonctions Step Functions pour invoquer des fonctions Lambda](#)
- [Vérifiez une identité e-mail et envoyez des messages à Amazon SES à l'aide d'un AWS Kit SDK](#)

Exemples de base pour l'utilisation d'Amazon SES AWS Kits SDK

Les exemples de code suivants illustrent comment utiliser les principes de base d'Amazon Simple Email Service avec des kits AWS SDK.

Exemples

- [Actions pour Amazon SES utilisant AWS Kits SDK](#)
 - [À utiliser CreateReceiptFilteravec un AWS Kit SDK](#)
 - [À utiliser CreateReceiptRuleavec un AWS Kit SDK](#)
 - [À utiliser CreateReceiptRuleSetavec un AWS Kit SDK](#)
 - [À utiliser CreateTemplateavec un AWS Kit SDK](#)
 - [À utiliser DeleteIdentityavec un AWS SDK ou CLI](#)
 - [À utiliser DeleteReceiptFilteravec un AWS Kit SDK](#)
 - [À utiliser DeleteReceiptRuleavec un AWS Kit SDK](#)
 - [À utiliser DeleteReceiptRuleSetavec un AWS Kit SDK](#)
 - [À utiliser DeleteTemplateavec un AWS Kit SDK](#)
 - [À utiliser DescribeReceiptRuleSetavec un AWS Kit SDK](#)
 - [À utiliser GetIdentityVerificationAttributesavec un AWS SDK ou CLI](#)
 - [À utiliser GetSendQuotaavec un AWS SDK ou CLI](#)
 - [Utilisation de GetSendStatistics avec une CLI](#)
 - [À utiliser GetTemplateavec un AWS Kit SDK](#)
 - [À utiliser ListIdentitiesavec un AWS SDK ou CLI](#)
 - [À utiliser ListReceiptFiltersavec un AWS Kit SDK](#)
 - [À utiliser ListTemplatesavec un AWS Kit SDK](#)

- [À utiliser SendBulkTemplatedEmailavec un AWS Kit SDK](#)
- [À utiliser SendEmailavec un AWS SDK ou CLI](#)
- [À utiliser SendRawEmailavec un AWS SDK ou CLI](#)
- [À utiliser SendTemplatedEmailavec un AWS Kit SDK](#)
- [À utiliser UpdateTemplateavec un AWS Kit SDK](#)
- [À utiliser VerifyDomainIdentityavec un AWS SDK ou CLI](#)
- [À utiliser VerifyEmailIdentityavec un AWS SDK ou CLI](#)

Actions pour Amazon SES utilisant AWS Kits SDK

Les exemples de code suivants montrent comment effectuer des actions Amazon SES individuelles à l'aide des AWS SDK. Chaque exemple inclut un lien vers GitHub, où vous pouvez trouver des instructions pour configurer et exécuter le code.

Ces extraits appellent l'API Amazon SES et sont des extraits de code de programmes plus volumineux qui doivent être exécutés en contexte. Vous pouvez voir les actions dans leur contexte dans [Scénarios d'utilisation d'Amazon SES AWS Kits SDK](#).

Les exemples suivants incluent uniquement les actions les plus couramment utilisées. Pour une description complète, consultez le document [Référence de l'API Amazon Simple Email Service](#).

Exemples

- [À utiliser CreateReceiptFilteravec un AWS Kit SDK](#)
- [À utiliser CreateReceiptRuleavec un AWS Kit SDK](#)
- [À utiliser CreateReceiptRuleSetavec un AWS Kit SDK](#)
- [À utiliser CreateTemplateavec un AWS Kit SDK](#)
- [À utiliser DeleteIdentityavec un AWS SDK ou CLI](#)
- [À utiliser DeleteReceiptFilteravec un AWS Kit SDK](#)
- [À utiliser DeleteReceiptRuleavec un AWS Kit SDK](#)
- [À utiliser DeleteReceiptRuleSetavec un AWS Kit SDK](#)
- [À utiliser DeleteTemplateavec un AWS Kit SDK](#)
- [À utiliser DescribeReceiptRuleSetavec un AWS Kit SDK](#)
- [À utiliser GetIdentityVerificationAttributesavec un AWS SDK ou CLI](#)
- [À utiliser GetSendQuotaavec un AWS SDK ou CLI](#)

- [Utilisation de GetSendStatistics avec une CLI](#)
- [À utiliser GetTemplateavec un AWS Kit SDK](#)
- [À utiliser ListIdentitiesavec un AWS SDK ou CLI](#)
- [À utiliser ListReceiptFiltersavec un AWS Kit SDK](#)
- [À utiliser ListTemplatesavec un AWS Kit SDK](#)
- [À utiliser SendBulkTemplatedEmailavec un AWS Kit SDK](#)
- [À utiliser SendEmailavec un AWS SDK ou CLI](#)
- [À utiliser SendRawEmailavec un AWS SDK ou CLI](#)
- [À utiliser SendTemplatedEmailavec un AWS Kit SDK](#)
- [À utiliser UpdateTemplateavec un AWS Kit SDK](#)
- [À utiliser VerifyDomainIdentityavec un AWS SDK ou CLI](#)
- [À utiliser VerifyEmailIdentityavec un AWS SDK ou CLI](#)

À utiliser **CreateReceiptFilter**avec un AWS Kit SDK

Les exemples de code suivants illustrent 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 [CreateReceiptFilter](#) à la section Référence des AWS SDK pour 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 [CreateReceiptFilter](#) à la section Référence des AWS SDK pour JavaScript API.

Python

Kit SDK for 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 [CreateReceiptFilter](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```

" iv_allow = abap_true means 'Allow', abap_false means 'Block'
DATA(lv_policy) = COND /aws1/sesreceiptfilterpolicy(
    WHEN iv_allow = abap_true THEN 'Allow'
    ELSE 'Block'
).

```

```

DATA(lo_ip_filter) = NEW /aws1/cl_sesreceiptfilter(
    iv_policy = lv_policy
    iv_cidr = iv_ip_address_or_range
).

DATA(lo_filter) = NEW /aws1/cl_sesreceiptfilter(
    iv_name = iv_filter_name
    io_ipfilter = lo_ip_filter
).

TRY.
    lo_ses->createreceiptfilter( io_filter = lo_filter ).
    MESSAGE 'Receipt filter created successfully' TYPE 'I'.
CATCH /aws1/cx_sesalreadyexistsex INTO DATA(lo_ex1).
    DATA(lv_error) = |Filter already exists: { lo_ex1->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex1.
CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).
    lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex_generic.
ENDTRY.

```

- Pour plus de détails sur l'API, reportez-vous [CreateReceiptFilter](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **CreateReceiptRule** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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 [CreateReceiptRule](#) à la section Référence des AWS SDK pour 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 [CreateReceiptRule](#) à la section Référence des AWS SDK pour JavaScript API.

Python

Kit SDK for 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 [CreateReceiptRule](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

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 S3 action for copying emails to S3
DATA(lo_s3_action) = NEW /aws1/cl_sess3action(
    iv_bucketname = iv_bucket_name
    iv_objectkeyprefix = iv_prefix
).

" Create receipt action with S3 action
DATA(lo_action) = NEW /aws1/cl_sesreceiptaction(
    io_s3action = lo_s3_action
).

" Create list of actions
DATA lt_actions TYPE /aws1/cl_sesreceiptaction=>tt_receiptactionslist.
APPEND lo_action TO lt_actions.

" Create receipt rule
DATA(lo_rule) = NEW /aws1/cl_sesrecepiptrule(
    iv_name = iv_rule_name
    iv_enabled = abap_true
    it_recipients = it_recipients
    it_actions = lt_actions
).

TRY.
    lo_ses->createrecepiptrule(
        iv_rulesetname = iv_rule_set_name
        io_rule = lo_rule
    ).
    MESSAGE 'Receipt rule created successfully' TYPE 'I'.
CATCH /aws1/cx_sesinvalids3confex INTO DATA(lo_ex1).
    DATA(lv_error) = |Invalid S3 configuration: { lo_ex1->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
```

```

        RAISE EXCEPTION lo_ex1.
    CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).
        lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.
        MESSAGE lv_error TYPE 'I'.
        RAISE EXCEPTION lo_ex_generic.
    ENDTRY.

```

- Pour plus de détails sur l'API, reportez-vous [CreateReceiptRule](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **CreateReceiptRuleSet** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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, reportez-vous [CreateReceiptRuleSet](#) à la section Référence des AWS SDK pour 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, reportez-vous [CreateReceiptRuleSet](#) à la section Référence des AWS SDK pour JavaScript API.

Python

Kit SDK for 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 [CreateReceiptRuleSet](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```

TRY.
    lo_ses->createreceiptruleset( iv_rulesetname = iv_rule_set_name ).
    MESSAGE 'Receipt rule set created successfully' TYPE 'I'.
CATCH /aws1/cx_sesalreadyexistsex INTO DATA(lo_ex1).
    DATA(lv_error) = |Rule set already exists: { lo_ex1->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex1.
CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).
    lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex_generic.
ENDTRY.

```

- Pour plus de détails sur l'API, reportez-vous [CreateReceiptRuleSet](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **CreateTemplate** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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

SDK pour .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, reportez-vous [CreateTemplate](#) à la section Référence des AWS SDK pour .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, reportez-vous [CreateTemplate](#) à la section Référence des AWS SDK pour 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, reportez-vous [CreateTemplate](#) à la section Référence des AWS SDK pour JavaScript API.

Python

Kit SDK for 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 [CreateTemplate](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```
DATA(lo_template) = NEW /aws1/cl_sesemplate(  
    iv_templatename = iv_name  
    iv_subjectpart = iv_subject  
    iv_textpart = iv_text  
    iv_htmlpart = iv_html  
).  
  
TRY.  
    lo_ses->createtemplate( io_template = lo_template ).  
    MESSAGE 'Template created successfully' TYPE 'I'.  
CATCH /aws1/cx_sesalreadyexistsex INTO DATA(lo_ex1).  
    DATA(lv_error) = |Template already exists: { lo_ex1->get_text( ) }|.  
    MESSAGE lv_error TYPE 'I'.  
    RAISE EXCEPTION lo_ex1.  
CATCH /aws1/cx_sesinvalidtemplateex INTO DATA(lo_ex2).  
    lv_error = |Invalid template: { lo_ex2->get_text( ) }|.  
    MESSAGE lv_error TYPE 'I'.  
    RAISE EXCEPTION lo_ex2.  
CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).  
    lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.  
    MESSAGE lv_error TYPE 'I'.  
    RAISE EXCEPTION lo_ex_generic.  
ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous [CreateTemplate](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **DeleteIdentity** avec un AWS SDK ou CLI

Les exemples de code suivants illustrent 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 les exemples de code suivants :

- [Configuration des services d'envoi d'e-mails](#)
- [Vérifier une identité d'e-mail et envoyer des messages](#)

.NET

SDK pour .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, reportez-vous [DeleteIdentity](#) à la section Référence des AWS SDK pour .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, reportez-vous [DeleteIdentity](#) à la section Référence des AWS SDK pour 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, reportez-vous [DeleteIdentity](#) à la 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, reportez-vous [DeleteIdentity](#) à la section Référence des AWS SDK pour JavaScript API.

Python

Kit SDK for 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 [DeleteIdentity](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```
TRY.  
    lo_ses->deleteidentity( iv_identity = iv_identity ).  
    MESSAGE 'Identity deleted successfully' TYPE 'I'.  
CATCH /aws1/cx_rt_generic INTO DATA(lo_ex).  
    DATA(lv_error) = |An error occurred: { lo_ex->get_text( ) }|.  
    MESSAGE lv_error TYPE 'I'.  
    RAISE EXCEPTION lo_ex.  
ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous [DeleteIdentity](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **DeleteReceiptFilter** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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, reportez-vous [DeleteReceiptFilter](#) à la section Référence des AWS SDK pour 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, reportez-vous [DeleteReceiptFilter](#) à la section Référence des AWS SDK pour JavaScript API.

Python

Kit SDK for 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 [DeleteReceiptFilter](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```
TRY.  
    lo_ses->deletereciptfilter( iv_filtername = iv_filter_name ).  
    MESSAGE 'Receipt filter deleted successfully' TYPE 'I'.  
CATCH /aws1/cx_rt_generic INTO DATA(lo_ex).  
    DATA(lv_error) = |An error occurred: { lo_ex->get_text( ) }|.  
    MESSAGE lv_error TYPE 'I'.  
    RAISE EXCEPTION lo_ex.  
ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous [DeleteReceiptFilter](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **DeleteReceiptRule** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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, reportez-vous [DeleteReceiptRule](#) à la section Référence des AWS SDK pour 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, reportez-vous [DeleteReceiptRule](#) à la section Référence des AWS SDK pour JavaScript API.

Python

Kit SDK for 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 [DeleteReceiptRule](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```
TRY.  
    lo_ses->deletereciptrule(  
        iv_rulesetname = iv_rule_set_name  
        iv_rulename = iv_rule_name  
    ).  
    MESSAGE 'Receipt rule deleted successfully' TYPE 'I'.  
CATCH /aws1/cx_sesrulesetdoesnotexist INTO DATA(lo_ex1).  
    DATA(lv_error) = |Rule set does not exist: { lo_ex1->get_text( ) }|.  
    MESSAGE lv_error TYPE 'I'.  
    RAISE EXCEPTION lo_ex1.  
CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).  
    lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.  
    MESSAGE lv_error TYPE 'I'.  
    RAISE EXCEPTION lo_ex_generic.  
ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous [DeleteReceiptRule](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser `DeleteReceiptRuleSet` avec un AWS Kit SDK

Les exemples de code suivants illustrent 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, reportez-vous [DeleteReceiptRuleSet](#) à la section Référence des AWS SDK pour 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, reportez-vous [DeleteReceiptRuleSet](#) à la section Référence des AWS SDK pour JavaScript API.

Python

Kit SDK for 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 [DeleteReceiptRuleSet](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```
TRY.  
    lo_ses->deletereciptruleset( iv_rulesetname = iv_rule_set_name ).  
    MESSAGE 'Receipt rule set deleted successfully' TYPE 'I'.  
CATCH /aws1/cx_sescannotdeleteex INTO DATA(lo_ex1).  
    DATA(lv_error) = |Cannot delete rule set: { lo_ex1->get_text( ) }|.  
    MESSAGE lv_error TYPE 'I'.  
    RAISE EXCEPTION lo_ex1.  
CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).  
    lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.  
    MESSAGE lv_error TYPE 'I'.  
    RAISE EXCEPTION lo_ex_generic.  
ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous [DeleteReceiptRuleSet](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **DeleteTemplate** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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

SDK pour .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, reportez-vous [DeleteTemplate](#) à la section Référence des AWS SDK pour .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, reportez-vous [DeleteTemplate](#) à la section Référence des AWS SDK pour 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, reportez-vous [DeleteTemplate](#) à la section Référence des AWS SDK pour JavaScript API.

Python

Kit SDK for 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 [DeleteTemplate](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```

TRY.
    lo_ses->deletetemplate( iv_templatename = iv_template_name ).
    MESSAGE 'Template deleted successfully' TYPE 'I'.
CATCH /aws1/cx_rt_generic INTO DATA(lo_ex).
    DATA(lv_error) = |An error occurred: { lo_ex->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex.
ENDTRY.

```

- Pour plus de détails sur l'API, reportez-vous [DeleteTemplate](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **DescribeReceiptRuleSet** avec un AWS Kit SDK

Les exemples de code suivants illustrent comment utiliser `DescribeReceiptRuleSet`.

Python

Kit SDK for 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 [DescribeReceiptRuleSet](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```
TRY.  
    oo_result = lo_ses->describereceiptruleset(  
        iv_rulesetname = iv_rule_set_name  
    ).  
    MESSAGE 'Receipt rule set described successfully' TYPE 'I'.  
CATCH /aws1/cx_sesrulesetdoesnotexist INTO DATA(lo_ex1).  
    DATA(lv_error) = |Rule set does not exist: { lo_ex1->get_text( ) }|.  
    MESSAGE lv_error TYPE 'I'.  
    RAISE EXCEPTION lo_ex1.  
CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).  
    lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.  
    MESSAGE lv_error TYPE 'I'.  
    RAISE EXCEPTION lo_ex_generic.  
ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous [DescribeReceiptRuleSet](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **GetIdentityVerificationAttributes** avec un AWS SDK ou CLI

Les exemples de code suivants illustrent 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 les exemples de code suivants :

- [Configuration des services d'envoi d'e-mails](#)
- [Vérifier une identité d'e-mail et envoyer des messages](#)

.NET

SDK pour .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, reportez-vous [GetIdentityVerificationAttributes](#) à la section Référence des AWS SDK pour .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, reportez-vous [GetIdentityVerificationAttributes](#) à la section Référence des AWS CLI commandes.

Python

Kit SDK for 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 [GetIdentityVerificationAttributes](#) le 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
puts email if status == 'Success'
end

```

- Pour plus de détails sur l'API, reportez-vous [GetIdentityVerificationAttributes](#) à la section Référence des AWS SDK pour Ruby API.

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```

DATA lt_identities TYPE /aws1/cl_sesidentitylist_w=>tt_identitylist.
APPEND NEW /aws1/cl_sesidentitylist_w( iv_value = iv_identity ) TO
lt_identities.

TRY.
  DATA(lo_result) = lo_ses->getidentityverificationattrs(
    it_identities = lt_identities
  ).

  DATA(lt_attrs) = lo_result->get_verificationattributes( ).
  IF lt_attrs IS NOT INITIAL.
    LOOP AT lt_attrs ASSIGNING FIELD-SYMBOL(<ls_attr>).
      ov_status = <ls_attr>-value->get_verificationstatus( ).
      EXIT.
    ENDLLOOP.
  ELSE.
    ov_status = 'NotFound'.
  ENDIF.

```

```
ENDIF.  
CATCH /aws1/cx_rt_generic INTO DATA(lo_ex).  
  DATA(lv_error) = |An error occurred: { lo_ex->get_text( ) }|.  
  MESSAGE lv_error TYPE 'I'.  
  RAISE EXCEPTION lo_ex.  
ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous [GetIdentityVerificationAttributes](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **GetSendQuota** avec un AWS SDK ou CLI

Les exemples de code suivants illustrent comment utiliser GetSendQuota.

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 :

- [Configuration des services d'envoi d'e-mails](#)

.NET

SDK pour .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, reportez-vous [GetSendQuota](#) à la section Référence des AWS SDK pour .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
}
```

```
}
```

Max24HourSend est votre quota d'envoi, qui est 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 dernières 24 heures.

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, reportez-vous [GetSendQuota](#) à la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell V4

Exemple 1 : cette commande renvoie les limites d'envoi actuelles de l'utilisateur.

```
Get-SESSendQuota
```

- Pour plus de détails sur l'API, reportez-vous [GetSendQuota](#) à la section Référence des Outils AWS pour PowerShell applets de commande (V4).

Outils pour PowerShell V5

Exemple 1 : cette commande renvoie les limites d'envoi actuelles de l'utilisateur.

```
Get-SESSendQuota
```

- Pour plus de détails sur l'API, reportez-vous [GetSendQuota](#) à la section Référence des Outils AWS pour PowerShell applets de commande (V5).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utilisation de **GetSendStatistics** avec une CLI

Les exemples de code suivants illustrent comment utiliser `GetSendStatistics`.

CLI

AWS CLI

Pour obtenir vos statistiques d'envoi Amazon SES

L'exemple suivant utilise la commande `get-send-statistics` pour renvoyer vos limites 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 de l'activité d'envoi. Chaque point de données de la liste contient des statistiques pour un intervalle de 15 minutes.

Cet exemple ne comprend 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 [Monitoring Your Amazon SES Usage Statistics](#) dans le Manuel du développeur Amazon Simple Email Service.

- Pour plus de détails sur l'API, reportez-vous [GetSendStatistics](#) à la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell V4

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 de l'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, reportez-vous [GetSendStatistics](#) à la section Référence des Outils AWS pour PowerShell applets de commande (V4).

Outils pour PowerShell V5

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 de l'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, reportez-vous [GetSendStatistics](#) à la section Référence des Outils AWS pour PowerShell applets de commande (V5).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **GetTemplate** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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, reportez-vous [GetTemplate](#) à la section Référence des AWS SDK pour 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, reportez-vous [GetTemplate](#) à la section Référence des AWS SDK pour JavaScript API.

Python

Kit SDK for 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 [GetTemplate](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```
TRY.  
    DATA(lo_result) = lo_ses->gettemplate( iv_templatename =  
iv_template_name ).  
    oo_template = lo_result->get_template( ).  
    MESSAGE 'Template retrieved successfully' TYPE 'I'.  
CATCH /aws1/cx_sestmpldoesnotexistex INTO DATA(lo_ex1).  
    DATA(lv_error) = |Template does not exist: { lo_ex1->get_text( ) }|.  
    MESSAGE lv_error TYPE 'I'.  
    RAISE EXCEPTION lo_ex1.  
CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).  
    lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.  
    MESSAGE lv_error TYPE 'I'.  
    RAISE EXCEPTION lo_ex_generic.  
ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous [GetTemplate](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **ListIdentities** avec un AWS SDK ou CLI

Les exemples de code suivants illustrent 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](#)
- [Configuration des services d'envoi d'e-mails](#)
- [Vérifier une identité d'e-mail et envoyer des messages](#)

.NET

SDK pour .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, reportez-vous [ListIdentities](#) à la section Référence des AWS SDK pour .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, reportez-vous [ListIdentities](#) à la section Référence des AWS SDK pour C++ API.

CLI

AWS CLI

Pour répertorier toutes les identités (adresses e-mail et domaines) associées à 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, reportez-vous [ListIdentities](#) à la 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();

        listSESIIdentities(client);
    }

    public static void listSESIIdentities(SesClient client) {
        try {
            ListIdentitiesResponse identitiesResponse = client.listIdentities();
            List<String> identities = identitiesResponse.getIdentities();
            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, reportez-vous [ListIdentities](#) à la 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, reportez-vous [ListIdentities](#) à la section Référence des AWS SDK pour JavaScript API.

PowerShell

Outils pour PowerShell V4

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-SESIIdentity
```

- Pour plus de détails sur l'API, reportez-vous [ListIdentities](#) à la section Référence des Outils AWS pour PowerShell applets de commande (V4).

Outils pour PowerShell V5

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-SESIIdentity
```

- Pour plus de détails sur l'API, reportez-vous [ListIdentities](#) à la section Référence des Outils AWS pour PowerShell applets de commande (V5).

Python

Kit SDK for 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 [ListIdentities](#) le 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
  puts email if status == 'Success'
end
```

- Pour plus de détails sur l'API, reportez-vous [ListIdentities](#) à la section Référence des AWS SDK pour Ruby API.

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```
TRY.
  DATA(lo_result) = lo_ses->listidentities(
    iv_identitytype = iv_identity_type
    iv_maxitems     = iv_max_items
  ).
  ot_identities = lo_result->get_identities( ).
  MESSAGE 'Identities retrieved successfully' TYPE 'I'.
CATCH /aws1/cx_rt_generic INTO DATA(lo_ex).
  DATA(lv_error) = |An error occurred: { lo_ex->get_text( ) }|.
  MESSAGE lv_error TYPE 'I'.
  RAISE EXCEPTION lo_ex.
ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous [ListIdentities](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **ListReceiptFilters** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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, reportez-vous [ListReceiptFilters](#) à la section Référence des AWS SDK pour 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, reportez-vous [ListReceiptFilters](#) à la section Référence des AWS SDK pour JavaScript API.

Python

Kit SDK for 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 [ListReceiptFilters](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```
TRY.  
    DATA(lo_result) = lo_ses->listreceiptfilters( ).  
    ot_filters = lo_result->get_filters( ).  
    MESSAGE 'Receipt filters retrieved successfully' TYPE 'I'.  
CATCH /aws1/cx_rt_generic INTO DATA(lo_ex).  
    DATA(lv_error) = |An error occurred: { lo_ex->get_text( ) }|.  
    MESSAGE lv_error TYPE 'I'.  
    RAISE EXCEPTION lo_ex.  
ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous [ListReceiptFilters](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **ListTemplates** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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

SDK pour .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, reportez-vous [ListTemplates](#) à la section Référence des AWS SDK pour .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, reportez-vous [ListTemplates](#) à la 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, reportez-vous [ListTemplates](#) à la section Référence des AWS SDK pour JavaScript API.

Python

Kit SDK for 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 [ListTemplates](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

TRY.

```

    DATA(lo_result) = lo_ses->listtemplates( iv_maxitems = iv_max_items ).
    ot_templates = lo_result->get_templatesmetadata( ).
    MESSAGE 'Templates retrieved successfully' TYPE 'I'.
CATCH /aws1/cx_rt_generic INTO DATA(lo_ex).
    DATA(lv_error) = |An error occurred: { lo_ex->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex.

```

ENDTRY.

- Pour plus de détails sur l'API, reportez-vous [ListTemplates](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **SendBulkTemplatedEmail** avec un AWS Kit SDK

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, reportez-vous [SendBulkTemplatedEmail](#) à la section Référence des AWS SDK pour JavaScript API.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **SendEmail** avec un AWS SDK ou CLI

Les exemples de code suivants illustrent 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 les exemples de code suivants :

- [Configuration des services d'envoi d'e-mails](#)
- [Vérifier une identité d'e-mail et envoyer des messages](#)

.NET

SDK pour .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, reportez-vous [SendEmail](#) à la section Référence des AWS SDK pour .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, reportez-vous [SendEmail](#) à la section Référence des AWS SDK pour 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, reportez-vous [SendEmail](#) à la 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.printStackTrace();
    }
}

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.printStackTrace();
}
}

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, reportez-vous [SendEmail](#) à la 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, reportez-vous [SendEmail](#) à la section Référence des AWS SDK pour JavaScript API.

Python

Kit SDK for 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 [SendEmail](#) le 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>.'
```

```

    },
    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 => e
  puts "Email not sent. Error message: #{e}"
end

```

- Pour plus de détails sur l'API, reportez-vous [SendEmail](#) à la section Référence des AWS SDK pour Ruby API.

SAP ABAP

Kit SDK pour SAP ABAP

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 message object
DATA(lo_subject) = NEW /aws1/cl_sescontent( iv_data = iv_subject ).
DATA(lo_text_body) = NEW /aws1/cl_sescontent( iv_data = iv_text ).
DATA(lo_html_body) = NEW /aws1/cl_sescontent( iv_data = iv_html ).
DATA(lo_body) = NEW /aws1/cl_sesbody(
  io_text = lo_text_body
  io_html = lo_html_body
).
DATA(lo_message) = NEW /aws1/cl_sesmessage(
  io_subject = lo_subject
  io_body = lo_body
).

TRY.

```

```

" Send email
DATA(lo_result) = lo_ses->sendemail(
  iv_source = iv_source
  io_destination = io_destination
  io_message = lo_message
  it_replytoaddresses = it_reply_tos
).
ov_msg_id = lo_result->get_messageid( ).
MESSAGE 'Email sent successfully' TYPE 'I'.
CATCH /aws1/cx_sesacctssendingpause00 INTO DATA(lo_ex1).
  DATA(lv_error) = |Account sending paused: { lo_ex1->get_text( ) }|.
  MESSAGE lv_error TYPE 'I'.
  RAISE EXCEPTION lo_ex1.
CATCH /aws1/cx_sesmessagerejected INTO DATA(lo_ex2).
  lv_error = |Message rejected: { lo_ex2->get_text( ) }|.
  MESSAGE lv_error TYPE 'I'.
  RAISE EXCEPTION lo_ex2.
CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).
  lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.
  MESSAGE lv_error TYPE 'I'.
  RAISE EXCEPTION lo_ex_generic.
ENDTRY.

```

- Pour plus de détails sur l'API, reportez-vous [SendEmail](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **SendRawEmail** avec un AWS SDK ou CLI

Les exemples de code suivants illustrent 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\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 pour `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, reportez-vous [SendRawEmail](#) à la 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, reportez-vous [SendRawEmail](#) à la section Référence des AWS SDK pour JavaScript API.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **SendTemplatedEmail** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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

SDK pour .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, reportez-vous [SendTemplatedEmail](#) à la section Référence des AWS SDK pour .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, reportez-vous [SendTemplatedEmail](#) à la section Référence des AWS SDK pour 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, reportez-vous [SendTemplatedEmail](#) à la 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, reportez-vous [SendTemplatedEmail](#) à la section Référence des AWS SDK pour JavaScript API.

Python

Kit SDK for 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 [SendTemplatedEmail](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```

TRY.
    " Send templated email
    DATA(lo_result) = lo_ses->sendtemplatedemail(
        iv_source = iv_source
        io_destination = io_destination
        iv_template = iv_template_name
        iv_templatedata = iv_template_data
        it_replytoaddresses = it_reply_tos
    ).
    ov_msg_id = lo_result->get_messageid( ).
    MESSAGE 'Templated email sent successfully' TYPE 'I'.
    CATCH /aws1/cx_sestmpldoesnotexistex INTO DATA(lo_ex1).
        DATA(lv_error) = |Template does not exist: { lo_ex1->get_text( ) }|.
        MESSAGE lv_error TYPE 'I'.
        RAISE EXCEPTION lo_ex1.
    CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).
        lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.
        MESSAGE lv_error TYPE 'I'.
        RAISE EXCEPTION lo_ex_generic.
ENDTRY.

```

- Pour plus de détails sur l'API, reportez-vous [SendTemplatedEmail](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **UpdateTemplate** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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, reportez-vous [UpdateTemplate](#) à la section Référence des AWS SDK pour 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, reportez-vous [UpdateTemplate](#) à la section Référence des AWS SDK pour JavaScript API.

Python

Kit SDK for 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 [UpdateTemplate](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```

DATA(lo_template) = NEW /aws1/cl_sestemplate(
    iv_templatename = iv_name
    iv_subjectpart = iv_subject
    iv_textpart = iv_text
    iv_htmlpart = iv_html
).

TRY.
    lo_ses->updatetemplate( io_template = lo_template ).
    MESSAGE 'Template updated successfully' TYPE 'I'.
CATCH /aws1/cx_sestmpldoesnotexistex INTO DATA(lo_ex1).
    DATA(lv_error) = |Template does not exist: { lo_ex1->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex1.
CATCH /aws1/cx_sesinvalidtemplateex INTO DATA(lo_ex2).
    lv_error = |Invalid template: { lo_ex2->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex2.
CATCH /aws1/cx_rt_generic INTO DATA(lo_ex_generic).
    lv_error = |An error occurred: { lo_ex_generic->get_text( ) }|.

```



```
MESSAGE lv_error TYPE 'I'.  
RAISE EXCEPTION lo_ex_generic.  
ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous [UpdateTemplate](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **VerifyDomainIdentity** avec un AWS SDK ou CLI

Les exemples de code suivants illustrent 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](#)
- [Configuration des services d'envoi d'e-mails](#)
- [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/wwwvjuEXAMPLE"
```

```
}
```

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, reportez-vous [VerifyDomainIdentity](#) à la 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, reportez-vous [VerifyDomainIdentity](#) à la section Référence des AWS SDK pour JavaScript API.

Python

Kit SDK for 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 [VerifyDomainIdentity](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```

TRY.
    DATA(lo_result) = lo_ses->verifydomainidentity( iv_domain =
iv_domain_name ).
    ov_token = lo_result->get_verificationtoken( ).
    MESSAGE 'Domain verification initiated' TYPE 'I'.
CATCH /aws1/cx_rt_generic INTO DATA(lo_ex).
    DATA(lv_error) = |An error occurred: { lo_ex->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex.
ENDTRY.

```

- Pour plus de détails sur l'API, reportez-vous [VerifyDomainIdentity](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **VerifyEmailIdentity** avec un AWS SDK ou CLI

Les exemples de code suivants illustrent 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](#)
- [Configuration des services d'envoi d'e-mails](#)
- [Vérifier une identité d'e-mail et envoyer des messages](#)

.NET

SDK pour .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, reportez-vous [VerifyEmailIdentity](#) à la section Référence des AWS SDK pour .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, reportez-vous [VerifyEmailIdentity](#) à la section Référence des AWS SDK pour 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 appelé `verify-email-identity`, 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, reportez-vous [VerifyEmailIdentity](#) à la 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, reportez-vous [VerifyEmailIdentity](#) à la section Référence des AWS SDK pour JavaScript API.

Python

Kit SDK for 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 [VerifyEmailIdentity](#) le 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
  })
end
```

```
puts "Email sent to #{recipient}"

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

- Pour plus de détails sur l'API, reportez-vous [VerifyEmailIdentity](#) à la section Référence des AWS SDK pour Ruby API.

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```
TRY.
    lo_ses->verifyemailidentity( iv_emailaddress = iv_email_address ).
    MESSAGE 'Email verification initiated' TYPE 'I'.
CATCH /aws1/cx_rt_generic INTO DATA(lo_ex).
    DATA(lv_error) = |An error occurred: { lo_ex->get_text( ) }|.
    MESSAGE lv_error TYPE 'I'.
    RAISE EXCEPTION lo_ex.
ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous [VerifyEmailIdentity](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Scénarios d'utilisation d'Amazon SES AWS Kits SDK

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 ou en les combinant avec d'autres Services AWS. Chaque exemple inclut un lien vers le code source complet, où vous trouverez des instructions sur la configuration et l'exécution du code.

Les scénarios ciblent un niveau d'expérience intermédiaire pour vous aider à comprendre les actions de service dans leur contexte.

Exemples

- [Créer une application de streaming Amazon Transcribe](#)
- [Copiez les adresses e-mail et de domaine d'Amazon SES à partir d'un AWS Région vers une autre à l'aide d'un AWS Kit SDK](#)
- [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](#)
- [Déterminez le PPE dans les images avec Amazon Rekognition à l'aide d'un AWS Kit SDK](#)
- [Déterminez des objets dans des images avec Amazon Rekognition à l'aide d'un AWS Kit SDK](#)
- [Déterminez les personnes et les objets dans une vidéo avec Amazon Rekognition à l'aide d'un AWS Kit SDK](#)
- [Générer des informations d'identification pour vous connecter à un point de terminaison d'un SMTP Amazon SES](#)
- [Configuration des services d'envoi d'e-mails](#)
- [Utiliser les fonctions Step Functions pour invoquer des fonctions Lambda](#)
- [Vérifiez une identité e-mail et envoyez des messages à Amazon SES à l'aide d'un AWS Kit SDK](#)

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, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Copiez les adresses e-mail et de domaine d'Amazon SES à partir d'un AWS Région vers une autre à l'aide d'un AWS Kit 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

Kit SDK for 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, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit 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

SDK pour .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

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 pour 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, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit 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, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit 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

SDK pour .NET

Montre comment utiliser le AWS SDK pour .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 intégré React.js pour interagir avec un backend .NET RESTful.

- 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 pour 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 intégré React.js pour interagir avec un Node.js backend Express.

- Intégrez une application React.js Web 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 pour 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 front-end intégré React.js pour interagir avec un backend PHP RESTful.

- Intégrez une application React.js Web 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 pour 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, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Détectez le PPE dans les images avec Amazon Rekognition à l'aide d'un AWS Kit SDK

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

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Détectez des objets dans des images avec Amazon Rekognition à l'aide d'un AWS Kit SDK

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

SDK pour .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 pour 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 pour 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, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Détectez les personnes et les objets dans une vidéo avec Amazon Rekognition à l'aide d'un AWS Kit SDK

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
- Amazon SNS
- Amazon SQS

Python

SDK pour Python (Boto3)

Utilisez Amazon Rekognition pour détecter des visages, des objets et des personnes dans des vidéos en démarrant des tâches de détection asynchrone. Cet exemple montre également comment configurer Amazon Rekognition pour notifier une rubrique Amazon Simple Notification Service (Amazon SNS) lorsque les tâches sont terminées et abonner une file d'attente Amazon Simple Queue Service (Amazon SQS) à la rubrique. Lorsque la file d'attente reçoit un message concernant une tâche, elle est récupérée et les résultats sont affichés.

Il est préférable de visionner cet exemple sur GitHub. 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
- Amazon SNS
- Amazon SQS

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit 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

Kit SDK for 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)
    "us-gov-east-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, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Configuration des services d'envoi d'e-mails

L'exemple de code suivant illustre comment :

- Vérifier une adresse e-mail
- Vérifier un domaine (facultatif)
- Vérifiez vos limites d'envoi
- Envoyer un e-mail de test
- nettoyer des ressources ;

Bash

AWS CLI avec le script Bash

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](#).

```
#!/bin/bash

# Amazon SES Setup Script (v2)
# This script helps you set up Amazon SES for sending emails

# Initialize log file
LOG_FILE="ses-setup.log"
echo "Starting Amazon SES setup at $(date)" > "$LOG_FILE"

# Function to log commands and their output
log_cmd() {
    echo "Running: $1" | tee -a "$LOG_FILE"
    eval "$1" 2>&1 | tee -a "$LOG_FILE"
    return ${PIPESTATUS[0]}
}

# Function to check for errors in command output
check_error() {
    local cmd_output="$1"
    local cmd_status="$2"
```

```

    local error_msg="$3"
    local ignore_error="${4:-false}"

    if [[ $cmd_status -ne 0 || "$cmd_output" =~ [Ee][Rr][Rr][Oo][Rr] ]]; then
        echo "ERROR: $error_msg" | tee -a "$LOG_FILE"
        if [[ "$ignore_error" != "true" ]]; then
            cleanup_resources
            exit 1
        fi
    fi
}

# Function to clean up resources
cleanup_resources() {
    echo "Cleaning up resources..." | tee -a "$LOG_FILE"

    # No physical resources to clean up for SES setup
    # Email identities can be deleted if needed
    if [[ -n "$EMAIL_ADDRESS" ]]; then
        echo "Deleting email identity: $EMAIL_ADDRESS" | tee -a "$LOG_FILE"
        log_cmd "aws ses delete-identity --identity \"$EMAIL_ADDRESS\""
    fi

    if [[ -n "$RECIPIENT_EMAIL" && "$RECIPIENT_EMAIL" != "$EMAIL_ADDRESS" ]];
then
        echo "Deleting recipient email identity: $RECIPIENT_EMAIL" | tee -a
"$LOG_FILE"
        log_cmd "aws ses delete-identity --identity \"$RECIPIENT_EMAIL\""
    fi

    if [[ -n "$DOMAIN_NAME" ]]; then
        echo "Deleting domain identity: $DOMAIN_NAME" | tee -a "$LOG_FILE"
        log_cmd "aws ses delete-identity --identity \"$DOMAIN_NAME\""
    fi
}

# Track created resources
CREATED_RESOURCES=()

# Welcome message
echo "=====
echo "Amazon SES Setup Script"
echo "=====
echo "This script will help you set up Amazon SES for sending emails."

```



```
echo "You'll need to verify at least one email address that you own."
echo ""
echo "NOTE: New SES accounts are placed in the sandbox environment."
echo "In the sandbox, both sender AND recipient email addresses must be
  verified."
echo ""

# Get email address to verify
echo "Please enter an email address that you own and can access:"
EMAIL_ADDRESS="user-$(cat /dev/urandom | tr -dc 'a-z0-9' | fold -w 8 | head -n
  1)@example.com"
echo "$EMAIL_ADDRESS"

# Verify email identity
echo "Verifying email address: $EMAIL_ADDRESS" | tee -a "$LOG_FILE"
OUTPUT=$(log_cmd "aws ses verify-email-identity --email-address \"$EMAIL_ADDRESS
  \")
check_error "$OUTPUT" $? "Failed to verify email address"

CREATED_RESOURCES+=("Email identity: $EMAIL_ADDRESS")
echo "A verification email has been sent to $EMAIL_ADDRESS."
echo "Please check your inbox and click the verification link before continuing."
echo ""
echo "Press Enter after you've verified your email address..."
sleep 1

# Check verification status
echo "Checking verification status..." | tee -a "$LOG_FILE"
OUTPUT=$(log_cmd "aws ses list-identities --identity-type EmailAddress")
check_error "$OUTPUT" $? "Failed to list identities"

OUTPUT=$(log_cmd "aws ses get-identity-verification-attributes --identities
  \"$EMAIL_ADDRESS\")
check_error "$OUTPUT" $? "Failed to get verification attributes"

# Check if the email is verified
VERIFICATION_STATUS=$(echo "$OUTPUT" | grep -o '"VerificationStatus": "[^"]*' |
  cut -d'"' -f4)
if [[ "$VERIFICATION_STATUS" != "Success" ]]; then
  echo "Email address $EMAIL_ADDRESS is not verified yet. Please check your
    inbox and verify before continuing."
  echo "Exiting script..."
  exit 1
fi
```

```

# Ask if user wants to verify a domain
echo ""
echo "Do you want to verify a domain for sending emails? (y/n):"
VERIFY_DOMAIN="y"
echo "$VERIFY_DOMAIN"

if [[ "$VERIFY_DOMAIN" =~ ^[Yy] ]]; then
    echo "Please enter the domain name you want to verify:"
    DOMAIN_NAME="test-$(cat /dev/urandom | tr -dc 'a-z0-9' | fold -w 8 | head -n
1).example.com"
    echo "$DOMAIN_NAME"

    # Verify domain identity
    echo "Verifying domain: $DOMAIN_NAME" | tee -a "$LOG_FILE"
    OUTPUT=$(log_cmd "aws ses verify-domain-identity --domain \"$DOMAIN_NAME\"")
    check_error "$OUTPUT" $? "Failed to verify domain identity"

    # Extract verification token
    VERIFICATION_TOKEN=$(echo "$OUTPUT" | grep -o '"VerificationToken": "[^"]*' |
cut -d'"' -f4)

    CREATED_RESOURCES+=("Domain identity: $DOMAIN_NAME")

    echo ""
    echo "======"
    echo "Domain Verification Instructions"
    echo "======"
    echo "To verify your domain ownership, you need to add a TXT record"
    echo "to your domain's DNS settings with the following values:"
    echo ""
    echo "Record Type: TXT"
    echo "Record Name: _amazonses.$DOMAIN_NAME"
    echo "Record Value: $VERIFICATION_TOKEN"
    echo ""
    echo "After adding this DNS record, verification may take up to 72 hours."
    echo ""

    # Set up DKIM for the domain
    echo "Setting up DKIM for domain: $DOMAIN_NAME" | tee -a "$LOG_FILE"
    OUTPUT=$(log_cmd "aws ses verify-domain-dkim --domain \"$DOMAIN_NAME\"")
    check_error "$OUTPUT" $? "Failed to set up DKIM"

    # Extract DKIM tokens

```

```

DKIM_TOKENS=$(echo "$OUTPUT" | grep -o '"DkimTokens": \[[^\]]*\]' | sed
's/"DkimTokens": \[[^\]]*\]/g' | sed 's/,//g' | sed 's/"//g')

echo "=====
echo "DKIM Configuration Instructions"
echo "=====
echo "To configure DKIM for your domain, add the following CNAME records"
echo "to your domain's DNS settings:"
echo ""

for token in $DKIM_TOKENS; do
    echo "Record Type: CNAME"
    echo "Record Name: ${token}._domainkey.$DOMAIN_NAME"
    echo "Record Value: ${token}.dkim.amazonses.com"
    echo ""
done

echo "After adding these DNS records, DKIM verification may take up to 72
hours."
echo ""
fi

# Check sending limits
echo "Checking your SES sending limits..." | tee -a "$LOG_FILE"
OUTPUT=$(log_cmd "aws ses get-send-quota")
check_error "$OUTPUT" $? "Failed to get sending quota"

# Extract quota information
MAX_SEND_RATE=$(echo "$OUTPUT" | grep -o '"MaxSendRate": [0-9]*' | cut -d' ' -
f2)
MAX_24_HOUR_SEND=$(echo "$OUTPUT" | grep -o '"Max24HourSend": [0-9]*' | cut -d'
' -f2)
SENT_LAST_24_HOURS=$(echo "$OUTPUT" | grep -o '"SentLast24Hours": [0-9]*' | cut
-d' ' -f2)

echo ""
echo "=====
echo "Your SES Sending Limits"
echo "=====
echo "Maximum send rate: $MAX_SEND_RATE emails/second"
echo "Maximum 24-hour send: $MAX_24_HOUR_SEND emails"
echo "Sent in the last 24 hours: $SENT_LAST_24_HOURS emails"
echo ""

```

```

# Ask if user wants to send a test email
echo "Do you want to send a test email? (y/n):"
SEND_TEST="y"
echo "$SEND_TEST"

if [[ "$SEND_TEST" =~ ^[Yy] ]]; then
    echo ""
    echo "=====
    echo "SANDBOX ENVIRONMENT NOTICE"
    echo "=====
    echo "Your account is likely in the SES sandbox environment."
    echo "In the sandbox, you can only send emails to verified email addresses."
    echo ""
    echo "Do you want to:"
    echo "1. Send a test email to the same verified address ($EMAIL_ADDRESS)"
    echo "2. Verify another email address to use as recipient"
    echo ""
    echo "Enter your choice (1 or 2):"
    RECIPIENT_CHOICE="1"
    echo "$RECIPIENT_CHOICE"

    if [[ "$RECIPIENT_CHOICE" == "1" ]]; then
        RECIPIENT_EMAIL="$EMAIL_ADDRESS"
    else
        echo "Please enter the recipient email address you want to verify:"
        RECIPIENT_EMAIL="user-$(cat /dev/urandom | tr -dc 'a-z0-9' | fold -w 8 |
head -n 1)@example.com"
        echo "$RECIPIENT_EMAIL"

        # Verify recipient email identity if different from sender
        if [[ "$RECIPIENT_EMAIL" != "$EMAIL_ADDRESS" ]]; then
            echo "Verifying recipient email address: $RECIPIENT_EMAIL" | tee -a
"$LOG_FILE"
            OUTPUT=$(log_cmd "aws ses verify-email-identity --email-address
\"$RECIPIENT_EMAIL\"")
            check_error "$OUTPUT" $? "Failed to verify recipient email address"

            CREATED_RESOURCES+=("Email identity: $RECIPIENT_EMAIL")
            echo "A verification email has been sent to $RECIPIENT_EMAIL."
            echo "Please check the inbox and click the verification link before
continuing."
            echo ""
            echo "Press Enter after you've verified the recipient email
address..."

```

```

        sleep 1

        # Check recipient verification status
        OUTPUT=$(log_cmd "aws ses get-identity-verification-attributes --
identities \"\$RECIPIENT_EMAIL\"")
        check_error "$OUTPUT" $? "Failed to get recipient verification
attributes"

        # Check if the recipient email is verified
        RECIPIENT_VERIFICATION_STATUS=$(echo "$OUTPUT" | grep -o
'"VerificationStatus": "[^"]*' | cut -d'"' -f4)
        if [[ "$RECIPIENT_VERIFICATION_STATUS" != "Success" ]]; then
            echo "Recipient email address $RECIPIENT_EMAIL is not verified
yet."
            echo "You can try sending the email anyway, but it may fail."
        fi
    fi
fi

echo "Sending test email from $EMAIL_ADDRESS to $RECIPIENT_EMAIL..." | tee -a
"$LOG_FILE"
OUTPUT=$(log_cmd "aws ses send-email \
--from \"\$EMAIL_ADDRESS\" \
--destination \"ToAddresses=$RECIPIENT_EMAIL\" \
--message \"Subject={Data=SES Test
Email,Charset=UTF-8},Body={Text={Data=This is a test email sent from Amazon SES
using the AWS CLI,Charset=UTF-8}}\"")

# Don't exit on send email error, just report it
check_error "$OUTPUT" $? "Failed to send test email" "true"

# Check if the email was sent successfully
if [[ "$OUTPUT" =~ "MessageId" ]]; then
    # Extract message ID
    MESSAGE_ID=$(echo "$OUTPUT" | grep -o '"MessageId": "[^"]*' | cut -d'"' -
f4)
    echo "Test email sent successfully! Message ID: $MESSAGE_ID"
else
    echo "Failed to send test email. This is likely because your account is
in the sandbox environment."
    echo "In the sandbox, both sender AND recipient email addresses must be
verified."
fi
echo ""

```

```

fi

# Summary of created resources
echo ""
echo "=====
echo "Setup Complete - Resources Created"
echo "=====
for resource in "${CREATED_RESOURCES[@]}"; do
    echo "- $resource"
done
echo ""

# Ask if user wants to clean up resources
echo "=====
echo "CLEANUP CONFIRMATION"
echo "=====
echo "Do you want to clean up all created resources? (y/n):"
CLEANUP_CHOICE="y"
echo "$CLEANUP_CHOICE"

if [[ "$CLEANUP_CHOICE" =~ ^[Yy] ]]; then
    cleanup_resources
    echo "Cleanup completed."
else
    echo "Resources have been preserved."
fi

echo ""
echo "=====
echo "Amazon SES Setup Complete"
echo "=====
echo "For production use, you may need to request to be moved out of the SES
  sandbox."
echo "Visit the SES console and navigate to 'Account dashboard' to request
  production access."
echo ""
echo "Log file: $LOG_FILE"
echo "=====

```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des commandes de l'AWS CLI .
 - [DeleteIdentity](#)

- [GetIdentityVerificationAttributes](#)
- [GetSendQuota](#)
- [ListIdentities](#)
- [SendEmail](#)
- [VerifyDomainDkim](#)
- [VerifyDomainIdentity](#)
- [VerifyEmailIdentity](#)

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Utiliser les fonctions Step Functions pour invoquer des fonctions Lambda

L'exemple de code suivant montre 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

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Vérifiez une identité e-mail et envoyez des messages à Amazon SES à l'aide d'un AWS Kit 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

Kit SDK for 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 de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK for Python (Boto3).
 - [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, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit 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.

Les scénarios sont des exemples de code qui vous montrent comment accomplir des tâches spécifiques en appelant plusieurs fonctions au sein d'un même service ou combinés à d'autres Services AWS.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

API Amazon SES v2

- [Exemples de base d'utilisation de l'API Amazon SES v2 AWS Kits SDK](#)
- [Bonjour Amazon SES API v2](#)
- [Actions pour l'API Amazon SES v2 à l'aide de AWS Kits SDK](#)
 - [À utiliser CreateContact avec un AWS Kit SDK](#)
 - [À utiliser CreateContactList avec un AWS Kit SDK](#)
 - [À utiliser CreateEmailIdentity avec un AWS Kit SDK](#)
 - [À utiliser CreateEmailTemplate avec un AWS Kit SDK](#)
 - [À utiliser DeleteContactList avec un AWS Kit SDK](#)
 - [À utiliser DeleteEmailIdentity avec un AWS Kit SDK](#)
 - [À utiliser DeleteEmailTemplate avec un AWS Kit SDK](#)
 - [À utiliser GetEmailIdentity avec un AWS Kit SDK](#)
 - [À utiliser ListContactLists avec un AWS Kit SDK](#)
 - [À utiliser ListContacts avec un AWS Kit SDK](#)
 - [À utiliser SendBulkEmail avec un AWS Kit SDK](#)
 - [À utiliser SendEmail avec un AWS Kit SDK](#)

- [Scénarios d'utilisation de l'API Amazon SES v2 AWS Kits SDK](#)
 - [Envoyer des e-mails avec des pièces jointes à l'aide de l'API Amazon SES v2](#)
 - [Un scénario complet de newsletter Amazon SES API v2 utilisant un AWS Kit SDK](#)

Exemples de base d'utilisation de l'API Amazon SES v2 AWS Kits SDK

Les exemples de code suivants illustrent comment utiliser les principes de base de l'API Amazon Simple Email Service v2 avec des kits AWS SDK.

Exemples

- [Bonjour Amazon SES API v2](#)
- [Actions pour l'API Amazon SES v2 à l'aide de AWS Kits SDK](#)
 - [À utiliser CreateContactavec un AWS Kit SDK](#)
 - [À utiliser CreateContactListavec un AWS Kit SDK](#)
 - [À utiliser CreateEmailIdentityavec un AWS Kit SDK](#)
 - [À utiliser CreateEmailTemplateavec un AWS Kit SDK](#)
 - [À utiliser DeleteContactListavec un AWS Kit SDK](#)
 - [À utiliser DeleteEmailIdentityavec un AWS Kit SDK](#)
 - [À utiliser DeleteEmailTemplateavec un AWS Kit SDK](#)
 - [À utiliser GetEmailIdentityavec un AWS Kit SDK](#)
 - [À utiliser ListContactListsavec un AWS Kit SDK](#)
 - [À utiliser ListContactsavec un AWS Kit SDK](#)
 - [À utiliser SendBulkEmailavec un AWS Kit SDK](#)
 - [À utiliser SendEmailavec un AWS Kit SDK](#)

Bonjour Amazon SES API v2

L'exemple de code suivant montre comment commencer à utiliser l'API Amazon SES v2.

Python

Kit SDK for 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](#).

```
def hello_sesv2(sesv2_client):
    """
    Use the AWS SDK for Python (Boto3) to create an Amazon SESv2 client and
    list the email identities in your account. This example uses the default
    settings specified in your shared credentials and config files.

    :param sesv2_client: A Boto3 SESv2 client object.
    """
    print("Hello, Amazon SESv2. Let's list up to 5 email identities:\n")

    try:
        response = sesv2_client.list_email_identities(PageSize=5)
        identities = response["EmailIdentities"]

        if not identities:
            print(
                "No email identities found. "
                "Use CreateEmailIdentity to add one."
            )
        else:
            for identity in identities:
                print(
                    f" Identity: {identity['IdentityName']}"
                    f" Type: {identity['IdentityType']}"
                    f" Status: {identity['VerificationStatus']}"
                    f" Sending: {'Enabled' if identity['SendingEnabled'] else
'Disabled'}"
                )
            print(f"\nShowing {len(identities)} email identity(ies).")

    except ClientError as err:
        logger.error(
```

```
        "Couldn't list email identities. Here's why: %s: %s",
        err.response["Error"]["Code"],
        err.response["Error"]["Message"],
    )
    raise
```

- Pour plus de détails sur l'API, consultez [ListEmailIdentities](#) le 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, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

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. Chaque exemple inclut un lien vers GitHub, où vous pouvez trouver des instructions pour configurer et exécuter le code.

Ces extraits appellent l'API Amazon SES v2 et sont des extraits de code de programmes plus volumineux qui doivent être exécutés en contexte. Vous pouvez voir les actions dans leur contexte dans [Scénarios d'utilisation de l'API Amazon SES v2 AWS Kits SDK](#).

Les exemples suivants incluent uniquement les actions les plus couramment utilisées. Pour une description complète, consultez le document [Référence de l'API Amazon Simple Email Service](#).

Exemples

- [À utiliser CreateContact avec un AWS Kit SDK](#)
- [À utiliser CreateContactList avec un AWS Kit SDK](#)
- [À utiliser CreateEmailIdentity avec un AWS Kit SDK](#)
- [À utiliser CreateEmailTemplate avec un AWS Kit SDK](#)
- [À utiliser DeleteContactList avec un AWS Kit SDK](#)
- [À utiliser DeleteEmailIdentity avec un AWS Kit SDK](#)
- [À utiliser DeleteEmailTemplate avec un AWS Kit SDK](#)
- [À utiliser GetEmailIdentity avec un AWS Kit SDK](#)

- [À utiliser ListContactLists avec un AWS Kit SDK](#)
- [À utiliser ListContacts avec un AWS Kit SDK](#)
- [À utiliser SendBulkEmail avec un AWS Kit SDK](#)
- [À utiliser SendEmail avec un AWS Kit SDK](#)

À utiliser **CreateContact** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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 :

- [Scénario de newsletter](#)

.NET

SDK pour .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>
/// 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 [CreateContact](#) à la section Référence des AWS SDK pour .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](#).

```
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()
    }.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 [CreateContact](#) à la section Référence des AWS SDK for Java 2.x API.

Python

Kit SDK for 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](#).

```

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 [CreateContact](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

Rust

SDK pour Rust

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](#).

```

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 [CreateContact](#) la section de référence de l'API AWS SDK for Rust.

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```
TRY.  
    lo_se2->createcontact(  
        iv_contactlistname = iv_contact_list_name  
        iv_emailaddress = iv_email_address ).  
    MESSAGE 'Contact created successfully.' TYPE 'I'.  
CATCH /aws1/cx_se2alreadyexistsex.  
    MESSAGE 'Contact already exists.' TYPE 'I'.  
CATCH /aws1/cx_se2badrequestex.  
    MESSAGE 'Bad request.' TYPE 'E'.  
CATCH /aws1/cx_se2notfoundexception.  
    MESSAGE 'Contact list not found.' TYPE 'E'.  
ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous [CreateContact](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **CreateContactList** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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 :

- [Scénario de newsletter](#)

.NET

SDK pour .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>
/// 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 [CreateContactList](#) à la section Référence des AWS SDK pour .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](#).

```
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 [CreateContactList](#) à la section Référence des AWS SDK for Java 2.x API.

Python

Kit SDK for 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](#).

```
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 [CreateContactList](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

Rust

SDK pour Rust

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](#).

```
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 [CreateContactList](#) la section de référence de l'API AWS SDK for Rust.

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```
TRY.  
    lo_se2->createcontactlist(  
        iv_contactlistname = iv_contact_list_name ).  
    MESSAGE 'Contact list created successfully.' TYPE 'I'.  
CATCH /aws1/cx_se2alreadyexistsex.  
    MESSAGE 'Contact list already exists.' TYPE 'I'.  
CATCH /aws1/cx_se2badrequestex INTO DATA(lo_bad_request).  
    MESSAGE 'Bad request - contact list limit may be reached.' TYPE 'I'.  
    " Re-raise the exception so the caller can handle it  
    RAISE EXCEPTION lo_bad_request.  
CATCH /aws1/cx_se2limitexceededex INTO DATA(lo_limit_exceeded).  
    MESSAGE 'Limit exceeded - contact list limit reached.' TYPE 'I'.  
    " Re-raise the exception so the caller can handle it  
    RAISE EXCEPTION lo_limit_exceeded.  
ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous [CreateContactList](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **CreateEmailIdentity** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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 les exemples de code suivants :

- [Scénario de pièces jointes aux e-mails](#)
- [Scénario de newsletter](#)

.NET

SDK pour .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>
/// 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 [CreateEmailIdentity](#) à la section Référence des AWS SDK pour .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](#).

```
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 [CreateEmailIdentity](#) à la section Référence des AWS SDK for Java 2.x API.

Python

Kit SDK for 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 SESv2Wrapper:
    """Encapsulates Amazon SESv2 email sending actions."""

    def __init__(self, sesv2_client: Any) -> None:
        """
        Initializes the SESv2Wrapper with an SESv2 client.

        :param sesv2_client: A Boto3 SESv2 client.
        """
        self.sesv2_client = sesv2_client

    @classmethod
    def from_client(cls) -> "SESv2Wrapper":
        """
        Creates an SESv2Wrapper instance with a default Boto3 SESv2 client.

        :return: A new SESv2Wrapper instance.
        """
        sesv2_client = boto3.client("sesv2")
        return cls(sesv2_client)

    def create_email_identity(self, email_address: str) -> Dict[str, Any]:
        """
        Starts the process of verifying an email identity (email address or
        domain).

        :param email_address: The email address or domain to verify.
        :return: A dictionary with the identity type and verification status.
        :raises ClientError: If the limit is exceeded (LimitExceededException).
        """
        try:
```



```

        response = self.sesv2_client.create_email_identity(
            EmailIdentity=email_address
        )
        logger.info(
            "Started verification for email identity %s.", email_address
        )
        return response
    except ClientError as err:
        if err.response["Error"]["Code"] == "LimitExceededException":
            logger.error(
                "Couldn't create email identity %s. You have exceeded "
                "the maximum number of email identities. "
                "Use an existing verified identity.",
                email_address,
            )
        else:
            logger.error(
                "Couldn't create email identity %s. Here's why: %s: %s",
                email_address,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
        raise

```

- Pour plus de détails sur l'API, consultez [CreateEmailIdentity](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

Kit SDK for 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](#).

```

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 [CreateEmailIdentity](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

Rust

SDK pour Rust

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](#).

```
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 [CreateEmailIdentity](#) la section de référence de l'API AWS SDK for Rust.

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```
TRY.  
    lo_se2->createemailidentity(  
        iv_emailidentity = iv_email_identity ).  
    MESSAGE 'Email identity created successfully.' TYPE 'I'.  
CATCH /aws1/cx_se2alreadyexistsex.  
    MESSAGE 'Email identity already exists.' TYPE 'I'.  
CATCH /aws1/cx_se2badrequestex INTO DATA(lo_bad_request).  
    MESSAGE lo_bad_request TYPE 'I' DISPLAY LIKE 'E'.  
CATCH /aws1/cx_se2limitexceededex INTO DATA(lo_limit_exceeded).  
    MESSAGE lo_limit_exceeded TYPE 'I' DISPLAY LIKE 'E'.  
ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous [CreateEmailIdentity](#) à la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **CreateEmailTemplate** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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 les exemples de code suivants :

- [Scénario de pièces jointes aux e-mails](#)
- [Scénario de newsletter](#)

.NET

SDK pour .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>
/// 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 [CreateEmailTemplate](#) à la section Référence des AWS SDK pour .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](#).

```
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 [CreateEmailTemplate](#) à la section Référence des AWS SDK for Java 2.x API.

Python

Kit SDK for 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 SESv2Wrapper:
    """Encapsulates Amazon SESv2 email sending actions."""

    def __init__(self, sesv2_client: Any) -> None:
        """
        Initializes the SESv2Wrapper with an SESv2 client.

        :param sesv2_client: A Boto3 SESv2 client.
        """
        self.sesv2_client = sesv2_client

    @classmethod
    def from_client(cls) -> "SESv2Wrapper":
        """
        Creates an SESv2Wrapper instance with a default Boto3 SESv2 client.

        :return: A new SESv2Wrapper instance.
        """
        sesv2_client = boto3.client("sesv2")
        return cls(sesv2_client)

    def create_email_template(
        self,
        template_name: str,
        subject: str,
        html_body: str,
        text_body: str,
    ) -> None:
        """
        Creates an email template for use with templated and bulk email sends.
```



```

        :param template_name: The name for the new template.
        :param subject: The subject line of the template. May include
        {{placeholders}}.
        :param html_body: The HTML body of the template.
        :param text_body: The plain text body of the template.
        :raises ClientError: If the template limit is exceeded
        (LimitExceededException).
        """
    try:
        self.sesv2_client.create_email_template(
            TemplateName=template_name,
            TemplateContent={
                "Subject": subject,
                "Html": html_body,
                "Text": text_body,
            },
        )
        logger.info("Created email template %s.", template_name)
    except ClientError as err:
        if err.response["Error"]["Code"] == "LimitExceededException":
            logger.error(
                "Couldn't create email template %s. You have exceeded "
                "the maximum number of email templates. "
                "Delete unused templates first.",
                template_name,
            )
        else:
            logger.error(
                "Couldn't create email template %s. Here's why: %s: %s",
                template_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
        raise

```

- Pour plus de détails sur l'API, consultez [CreateEmailTemplate](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

Kit SDK for 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](#).

```
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 [CreateEmailTemplate](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

Rust

SDK pour Rust

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](#).

```
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 [CreateEmailTemplate](#) la section de référence de l'API AWS SDK for Rust.

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

TRY.

```

DATA(lo_template_content) = NEW /aws1/cl_se2emailtmplcontent(
    iv_subject = iv_subject
    iv_html    = iv_html
    iv_text    = iv_text ).

```

```
lo_se2->createemailtemplate(  
    iv_templatename = iv_template_name  
    io_templatecontent = lo_template_content ).  
MESSAGE 'Email template created successfully.' TYPE 'I'.  
CATCH /aws1/cx_se2alreadyexistsex.  
    MESSAGE 'Email template already exists.' TYPE 'I'.  
CATCH /aws1/cx_se2badrequestex.  
    MESSAGE 'Bad request.' TYPE 'E'.  
CATCH /aws1/cx_se2limitexceededx.  
    MESSAGE 'Limit exceeded.' TYPE 'E'.  
ENDTRY.
```

- Pour plus de détails sur l'API, consultez [CreateEmailTemplate](#) la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **DeleteContactList** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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 :

- [Scénario de newsletter](#)

.NET

SDK pour .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>
/// 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 [DeleteContactList](#) à la section Référence des AWS SDK pour .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](#).

```
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 [DeleteContactList](#) à la section Référence des AWS SDK for Java 2.x API.

Python

Kit SDK for 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](#).

```
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 [DeleteContactList](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

Rust

SDK pour Rust

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](#).

```
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 [DeleteContactList](#) la section de référence de l'API AWS SDK for Rust.

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```
TRY.  
    lo_se2->deletecontactlist(  
        iv_contactlistname = iv_contact_list_name ).  
    MESSAGE 'Contact list deleted successfully.' TYPE 'I'.  
CATCH /aws1/cx_se2notfoundexception.  
    MESSAGE 'Contact list not found.' TYPE 'I'.  
CATCH /aws1/cx_se2badrequestex INTO DATA(lo_bad_request).  
    MESSAGE 'Bad request.' TYPE 'I'.  
    RAISE EXCEPTION lo_bad_request.  
ENDTRY.
```

- Pour plus de détails sur l'API, consultez [DeleteContactList](#) la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **DeleteEmailIdentity** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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 les exemples de code suivants :

- [Scénario de pièces jointes aux e-mails](#)
- [Scénario de newsletter](#)

.NET

SDK pour .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>
/// 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 [DeleteEmailIdentity](#) à la section Référence des AWS SDK pour .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](#).

```
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 [DeleteEmailIdentity](#) à la section Référence des AWS SDK for Java 2.x API.

Python

Kit SDK for 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 SESv2Wrapper:
    """Encapsulates Amazon SESv2 email sending actions."""

    def __init__(self, sesv2_client: Any) -> None:
        """
        Initializes the SESv2Wrapper with an SESv2 client.

        :param sesv2_client: A Boto3 SESv2 client.
        """
        self.sesv2_client = sesv2_client

    @classmethod
    def from_client(cls) -> "SESv2Wrapper":
        """
        Creates an SESv2Wrapper instance with a default Boto3 SESv2 client.

        :return: A new SESv2Wrapper instance.
        """
        sesv2_client = boto3.client("sesv2")

```

```
return cls(sesv2_client)

def delete_email_identity(self, email_address: str) -> None:
    """
    Deletes an email identity.

    :param email_address: The email address or domain to delete.
    :raises ClientError: If the identity is not found (NotFoundException).
    """
    try:
        self.sesv2_client.delete_email_identity(
            EmailIdentity=email_address
        )
        logger.info("Deleted email identity %s.", email_address)
    except ClientError as err:
        if err.response["Error"]["Code"] == "NotFoundException":
            logger.info(
                "Email identity %s not found or already deleted.",
                email_address,
            )
        else:
            logger.error(
                "Couldn't delete email identity %s. Here's why: %s: %s",
                email_address,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
        raise
```

- Pour plus de détails sur l'API, consultez [DeleteEmailIdentity](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

Kit SDK for 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](#).

```
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 [DeleteEmailIdentity](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

Rust

SDK pour Rust

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](#).

```
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 [DeleteEmailIdentity](#) la section de référence de l'API AWS SDK for Rust.

SAP ABAP

Kit SDK pour SAP ABAP

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](#).


```
TRY.  
    lo_se2->deleteemailidentity(  
        iv_emailidentity = iv_email_identity ).  
    MESSAGE 'Email identity deleted successfully.' TYPE 'I'.  
CATCH /aws1/cx_se2notfoundexception.  
    MESSAGE 'Email identity not found.' TYPE 'I'.  
CATCH /aws1/cx_se2badrequestex INTO DATA(lo_bad_request).  
    MESSAGE 'Bad request.' TYPE 'I'.  
    RAISE EXCEPTION lo_bad_request.  
ENDTRY.
```

- Pour plus de détails sur l'API, consultez [DeleteEmailIdentity](#) la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **DeleteEmailTemplate** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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 les exemples de code suivants :

- [Scénario de pièces jointes aux e-mails](#)
- [Scénario de newsletter](#)

.NET

SDK pour .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>
/// 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 [DeleteEmailTemplate](#) à la section Référence des AWS SDK pour .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](#).

```
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 [DeleteEmailTemplate](#) à la section Référence des AWS SDK for Java 2.x API.

Python

Kit SDK for 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 SESv2Wrapper:
    """Encapsulates Amazon SESv2 email sending actions."""

    def __init__(self, sesv2_client: Any) -> None:
        """
        Initializes the SESv2Wrapper with an SESv2 client.

        :param sesv2_client: A Boto3 SESv2 client.
        """
        self.sesv2_client = sesv2_client

    @classmethod
    def from_client(cls) -> "SESv2Wrapper":
        """
        Creates an SESv2Wrapper instance with a default Boto3 SESv2 client.

        :return: A new SESv2Wrapper instance.
        """
        sesv2_client = boto3.client("sesv2")
        return cls(sesv2_client)

    def delete_email_template(self, template_name: str) -> None:
        """
        Deletes an email template.

        :param template_name: The name of the template to delete.
        :raises ClientError: If the template is not found (NotFoundException).
        """
        try:
            self.sesv2_client.delete_email_template(
                TemplateName=template_name
```

```

    )
    logger.info("Deleted email template %s.", template_name)
except ClientError as err:
    if err.response["Error"]["Code"] == "NotFoundException":
        logger.info(
            "Email template %s not found or already deleted.",
            template_name,
        )
    else:
        logger.error(
            "Couldn't delete email template %s. Here's why: %s: %s",
            template_name,
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
    raise

```

- Pour plus de détails sur l'API, consultez [DeleteEmailTemplate](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

Kit SDK for 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](#).

```

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 [DeleteEmailTemplate](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

Rust

SDK pour Rust

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](#).

```

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 [DeleteEmailTemplate](#) la section de référence de l'API AWS SDK for Rust.

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```

TRY.
    lo_se2->deleteemailtemplate(
        iv_templatename = iv_template_name ).
    MESSAGE 'Email template deleted successfully.' TYPE 'I'.
CATCH /aws1/cx_se2notfoundexception.
    MESSAGE 'Email template not found.' TYPE 'I'.
CATCH /aws1/cx_se2badrequestex INTO DATA(lo_bad_request).
    MESSAGE 'Bad request.' TYPE 'I'.
    RAISE EXCEPTION lo_bad_request.
ENDTRY.

```

- Pour plus de détails sur l'API, consultez [DeleteEmailTemplate](#) la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **GetEmailIdentity** avec un AWS Kit SDK

Les exemples de code suivants illustrent comment utiliser `GetEmailIdentity`.

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 :

- [Scénario de pièces jointes aux e-mails](#)

Python

Kit SDK for 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 SESv2Wrapper:
    """Encapsulates Amazon SESv2 email sending actions."""

    def __init__(self, sesv2_client: Any) -> None:
        """
        Initializes the SESv2Wrapper with an SESv2 client.

        :param sesv2_client: A Boto3 SESv2 client.
        """
        self.sesv2_client = sesv2_client

    @classmethod
    def from_client(cls) -> "SESv2Wrapper":
        """
        Creates an SESv2Wrapper instance with a default Boto3 SESv2 client.

        :return: A new SESv2Wrapper instance.
```



```

    """
    sesv2_client = boto3.client("sesv2")
    return cls(sesv2_client)

    def get_email_identity(self, email_address: str) -> Dict[str, Any]:
        """
        Gets information about an email identity, including its verification
        status.

        :param email_address: The email address or domain to look up.
        :return: A dictionary with identity information including verification
        status.
        :raises ClientError: If the identity is not found (NotFoundException).
        """
        try:
            response = self.sesv2_client.get_email_identity(
                EmailIdentity=email_address
            )
            logger.info("Got email identity for %s.", email_address)
            return response
        except ClientError as err:
            if err.response["Error"]["Code"] == "NotFoundException":
                logger.info(
                    "Email identity %s not found.", email_address
                )
            else:
                logger.error(
                    "Couldn't get email identity %s. Here's why: %s: %s",
                    email_address,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
            raise

```

- Pour plus de détails sur l'API, consultez [GetEmailIdentity](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

Rust

SDK pour Rust

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](#).

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 [GetEmailIdentity](#) la section de référence de l'API AWS SDK for Rust.

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```

TRY.
    oo_result = lo_se2->getemailidentity(
        iv_emailidentity = iv_email_identity ).
    MESSAGE |Identity type: { oo_result->get_identitytype( ) }, | &&
        |verified for sending: { oo_result-
>get_verifiedforsendingstatus( ) }| TYPE 'I'.
    CATCH /aws1/cx_se2notfoundexception.
        MESSAGE |Email identity { iv_email_identity } not found.| TYPE 'I'.
    CATCH /aws1/cx_se2badrequestex INTO DATA(lo_bad_request).
        MESSAGE lo_bad_request TYPE 'I' DISPLAY LIKE 'E'.
        RAISE EXCEPTION lo_bad_request.
ENDTRY.

```

- Pour plus de détails sur l'API, consultez [GetEmailIdentity](#) la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **ListContactLists** avec un AWS Kit SDK

L'exemple de code suivant montre comment utiliser `ListContactLists`.

Rust

SDK pour Rust

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](#).

```

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 [ListContactLists](#) la 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, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **ListContacts** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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 :

- [Scénario de newsletter](#)

.NET

SDK pour .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>  
/// 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 [ListContacts](#) à la section Référence des AWS SDK pour .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](#).

```
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 [ListContacts](#) à la section Référence des AWS SDK for Java 2.x API.

Python

Kit SDK for 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](#).

```
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 [ListContacts](#) le AWS manuel de référence de l'API SDK for Python (Boto3).

Rust

SDK pour Rust

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](#).

```
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 [ListContacts](#) la section de référence de l'API AWS SDK for Rust.

SAP ABAP

Kit SDK pour SAP ABAP

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](#).


```
TRY.  
    oo_result = lo_se2->listcontacts(  
        iv_contactlistname = iv_contact_list_name ).  
    DATA(lv_count) = lines( oo_result->get_contacts( ) ).  
    MESSAGE |Retrieved { lv_count } contacts from list.| TYPE 'I'.  
CATCH /aws1/cx_se2badrequestex INTO DATA(lo_bad_request).  
    MESSAGE 'Bad request.' TYPE 'I'.  
    RAISE EXCEPTION lo_bad_request.  
CATCH /aws1/cx_se2notfoundexception INTO DATA(lo_not_found).  
    MESSAGE 'Contact list not found.' TYPE 'I'.  
    RAISE EXCEPTION lo_not_found.  
ENDTRY.
```

- Pour plus de détails sur l'API, consultez [ListContacts](#) la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **SendBulkEmail** avec un AWS Kit SDK

Les exemples de code suivants illustrent comment utiliser SendBulkEmail.

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 :

- [Scénario de pièces jointes aux e-mails](#)

Python

Kit SDK for 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 SESv2Wrapper:
    """Encapsulates Amazon SESv2 email sending actions."""

    def __init__(self, sesv2_client: Any) -> None:
        """
        Initializes the SESv2Wrapper with an SESv2 client.

        :param sesv2_client: A Boto3 SESv2 client.
        """
        self.sesv2_client = sesv2_client

    @classmethod
    def from_client(cls) -> "SESv2Wrapper":
        """
        Creates an SESv2Wrapper instance with a default Boto3 SESv2 client.

        :return: A new SESv2Wrapper instance.
        """
        sesv2_client = boto3.client("sesv2")
        return cls(sesv2_client)

    def send_bulk_email(
        self,
        from_address: str,
        template_name: str,
        default_template_data: str,
        bulk_entries: List[Dict[str, Any]],
        attachments: Optional[List[Dict[str, Any]]] = None,
    ) -> List[Dict[str, Any]]:
        """
        Sends a templated email to multiple recipients in a single API call.

        All recipients receive the same attachment(s) defined in the default
        content, while template data can be personalized per recipient.

        :param from_address: The verified sender email address.
        :param template_name: The name of an existing email template.
        :param default_template_data: Default JSON template data string.
        :param bulk_entries: A list of BulkEmailEntry dicts, each containing
            'Destination' and optionally 'ReplacementEmailContent'.
        :param attachments: An optional list of attachment dicts for all
            recipients.

```

```
:return: A list of BulkEmailEntryResult dicts with status and MessageId.
:raises ClientError: If the message is rejected (MessageRejected).
"""
try:
    template_content: Dict[str, Any] = {
        "TemplateName": template_name,
        "TemplateData": default_template_data,
    }

    if attachments:
        template_content["Attachments"] = attachments

    response = self.sesv2_client.send_bulk_email(
        FromEmailAddress=from_address,
        DefaultContent={"Template": template_content},
        BulkEmailEntries=bulk_entries,
    )
    results = response.get("BulkEmailEntryResults", [])
    logger.info(
        "Sent bulk email from %s to %d recipients.",
        from_address,
        len(bulk_entries),
    )
    return results
except ClientError as err:
    if err.response["Error"]["Code"] == "MessageRejected":
        logger.error(
            "Bulk message was rejected. Check that the template "
            "exists, attachment file types are supported, and "
            "total message size is within limits. Details: %s",
            err.response["Error"]["Message"],
        )
    else:
        logger.error(
            "Couldn't send bulk email. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
    raise
```

- Pour plus de détails sur l'API, consultez [SendBulkEmail](#) AWS manuel de référence de l'API SDK for Python (Boto3).

SAP ABAP

Kit SDK pour SAP ABAP

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](#).

```
TRY.
    " Build the default template content used for all bulk recipients
    DATA(lo_template) = NEW /aws1/cl_se2template(
        iv_templatename = iv_template_name
        iv_templatedata = iv_template_data ).

    DATA(lo_default_content) = NEW /aws1/cl_se2bulkemailcontent(
        io_template = lo_template ).

    DATA(lo_result) = lo_se2->sendbulkemail(
        iv_fromemailaddress = iv_from_address
        io_defaultcontent    = lo_default_content
        it_bulkemailentries = it_bulk_entries ).

    ot_results = lo_result->get_bulkemailentryresults( ).
    MESSAGE |Bulk email sent to { lines( it_bulk_entries ) } recipient(s).|
    TYPE 'I'.
    CATCH /aws1/cx_se2messagerejected INTO DATA(lo_rejected).
        MESSAGE lo_rejected TYPE 'I' DISPLAY LIKE 'E'.
        RAISE EXCEPTION lo_rejected.
    CATCH /aws1/cx_se2mailfrmdomnotver00 INTO DATA(lo_not_verified).
        MESSAGE lo_not_verified TYPE 'I' DISPLAY LIKE 'E'.
        RAISE EXCEPTION lo_not_verified.
    CATCH /aws1/cx_se2notfoundexception INTO DATA(lo_not_found).
        MESSAGE lo_not_found TYPE 'I' DISPLAY LIKE 'E'.
        RAISE EXCEPTION lo_not_found.
    CATCH /aws1/cx_se2badrequestex INTO DATA(lo_bad_request).
        MESSAGE lo_bad_request TYPE 'I' DISPLAY LIKE 'E'.
```

```
RAISE EXCEPTION lo_bad_request.  
ENDTRY.
```

- Pour plus de détails sur l'API, consultez [SendBulkEmail](#) la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

À utiliser **SendEmail** avec un AWS Kit SDK

Les exemples de code suivants illustrent 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 :

- [Scénario de pièces jointes aux e-mails](#)

.NET

SDK pour .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>  
/// 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 [SendEmail](#) à la section Référence des AWS SDK pour .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](#).

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.
    * <p>
    * For more information, see the following documentation topic:
    * <p>
    * 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());
    }

```

Envoie un message contenant des informations d'en-tête.

```

public class SendwithHeader {

    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();

    String bodyHTML = ""
        <html>
            <head></head>
            <body>
                <h1>Hello!</h1>
                <p>See the list of customers.</p>
            </body>
        </html>
        """;

    sendWithHeader(sesv2Client, sender, recipient, subject, bodyHTML);
    sesv2Client.close();
}

/**
 * Sends an email using the AWS SES V2 client.
 *
 * @param sesv2Client the SES V2 client to use for sending the email
 * @param sender the email address of the sender
 * @param recipient the email address of the recipient
 * @param subject the subject of the email
 * @param bodyHTML the HTML content of the email body
 */
public static void sendWithHeader(SesV2Client sesv2Client,
    String sender,

```

```

        String recipient,
        String subject,
        String bodyHTML) {
    EmailContent emailContent = EmailContent.builder()
        .simple(Message.builder()
            .body(b -> b.html(c ->
c.charset(UTF_8.name()).data(bodyHTML))
            .text(c ->
c.charset(UTF_8.name()).data(bodyHTML)))
            .subject(c -> c.charset(UTF_8.name()).data(subject))
            .headers(List.of(
                MessageHeader.builder()
                    .name("List-Unsubscribe")
                    .value("<https://nutrition.co/?
address=x&topic=x>, <mailto:unsubscribe@nutrition.co?subject=TopicUnsubscribe>")
                    .build(),
                MessageHeader.builder()
                    .name("List-Unsubscribe-Post")
                    .value("List-Unsubscribe=One-Click")
                    .build()))
            .build())
        .build();

    SendEmailRequest request = SendEmailRequest.builder()
        .fromEmailAddress(sender)
        .destination(d -> d.toAddresses(recipient))
        .content(emailContent)
        .build();

    try {
        SendEmailResponse response = sesv2Client.sendEmail(request);
        System.out.println("Email sent! Message ID: " +
response.messageId());
    } catch (SesV2Exception e) {
        System.err.println("Failed to send email: " +
e.awsErrorDetails().errorMessage());
        throw new RuntimeException(e);
    }
}
}

```

- Pour plus de détails sur l'API, reportez-vous [SendEmail](#) à la section Référence des AWS SDK for Java 2.x API.

Python

Kit SDK for 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](#).

Envoie un message avec des pièces jointes facultatives.

```
class SESv2Wrapper:
    """Encapsulates Amazon SESv2 email sending actions."""

    def __init__(self, sesv2_client: Any) -> None:
        """
        Initializes the SESv2Wrapper with an SESv2 client.

        :param sesv2_client: A Boto3 SESv2 client.
        """
        self.sesv2_client = sesv2_client

    @classmethod
    def from_client(cls) -> "SESv2Wrapper":
        """
        Creates an SESv2Wrapper instance with a default Boto3 SESv2 client.

        :return: A new SESv2Wrapper instance.
        """
        sesv2_client = boto3.client("sesv2")
        return cls(sesv2_client)

    def send_email(
        self,
        from_address: str,
        to_addresses: List[str],
        subject: str,
```

```

    html_body: str,
    text_body: str,
    attachments: Optional[List[Dict[str, Any]]] = None,
) -> str:
    """
    Sends a simple email message with optional attachments.

    SES handles MIME construction automatically when using attachments
    with the Simple content type, so developers don't need to build
    raw MIME messages.

    :param from_address: The verified sender email address.
    :param to_addresses: A list of recipient email addresses.
    :param subject: The subject line of the email.
    :param html_body: The HTML body content.
    :param text_body: The plain text body content.
    :param attachments: An optional list of attachment dictionaries. Each
        attachment should contain 'RawContent' (bytes), 'FileName' (str),
        and optionally 'ContentType', 'ContentDisposition', 'ContentId',
        'ContentDescription', and 'ContentTransferEncoding'.
    :return: The MessageId of the sent email.
    :raises ClientError: If the message is rejected (MessageRejected).
    """
    try:
        simple_message: Dict[str, Any] = {
            "Subject": {"Data": subject},
            "Body": {
                "Html": {"Data": html_body},
                "Text": {"Data": text_body},
            },
        }

        if attachments:
            simple_message["Attachments"] = attachments

        response = self.sesv2_client.send_email(
            FromEmailAddress=from_address,
            Destination={"ToAddresses": to_addresses},
            Content={"Simple": simple_message},
        )
        message_id = response["MessageId"]
        logger.info(
            "Sent email from %s to %s. MessageId: %s",
            from_address,

```

```

        to_addresses,
        message_id,
    )
    return message_id
except ClientError as err:
    if err.response["Error"]["Code"] == "MessageRejected":
        logger.error(
            "Message was rejected. Check that attachments use "
            "supported file types and total message size is "
            "under 40 MB. Details: %s",
            err.response["Error"]["Message"],
        )
    else:
        logger.error(
            "Couldn't send email. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
    raise

```

- Pour plus de détails sur l'API, consultez [SendEmail](#) AWS manuel de référence de l'API SDK for Python (Boto3).

Kit SDK for 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](#).

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 [SendEmail](#) le 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-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 [SendEmail](#) à la section Référence des AWS SDK pour Ruby API.

Rust

SDK pour Rust

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](#).

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 [SendEmail](#) la section de référence de l'API AWS SDK for Rust.

SAP ABAP

Kit SDK pour SAP ABAP

 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](#).

Envoie un message.

```

TRY.
    " Create destination with recipient address
    DATA lt_to_addresses TYPE /aws1/
cl_se2emailaddresslist_w=>tt_emailaddresslist.
    APPEND NEW /aws1/cl_se2emailaddresslist_w( iv_value =
iv_to_email_address ) TO lt_to_addresses.
    DATA(lo_destination) = NEW /aws1/cl_se2destination(
        it_toaddresses = lt_to_addresses ).

    " Create message content
    DATA(lo_subject) = NEW /aws1/cl_se2content( iv_data = iv_subject ).
    DATA(lo_text_body) = NEW /aws1/cl_se2content( iv_data = iv_text_body ).
    DATA(lo_html_body) = NEW /aws1/cl_se2content( iv_data = iv_html_body ).
    DATA(lo_body) = NEW /aws1/cl_se2body(
        io_text = lo_text_body
        io_html = lo_html_body ).
    DATA(lo_message) = NEW /aws1/cl_se2message(
        io_subject = lo_subject
        io_body = lo_body ).

    DATA(lo_content) = NEW /aws1/cl_se2emailcontent(
        io_simple = lo_message ).

    " Send the email
    lo_se2->sendemail(
        iv_fromemailaddress = iv_from_email_address
        io_destination = lo_destination
        io_content = lo_content ).
    MESSAGE 'Email sent successfully.' TYPE 'I'.
CATCH /aws1/cx_se2accountsuspendedex INTO DATA(lo_account_suspended).
    MESSAGE 'Account suspended.' TYPE 'I'.

```

```

        RAISE EXCEPTION lo_account_suspended.
    CATCH /aws1/cx_se2badrequestex INTO DATA(lo_bad_request).
        MESSAGE 'Bad request.' TYPE 'I'.
        RAISE EXCEPTION lo_bad_request.
    CATCH /aws1/cx_se2messagerejected INTO DATA(lo_message_rejected).
        MESSAGE 'Message rejected - check email verification.' TYPE 'I'.
        RAISE EXCEPTION lo_message_rejected.
ENDTRY.

```

Envoie un message à l'aide d'un modèle.

```

TRY.
    " Create destination with recipient address
    DATA lt_to_addresses TYPE /aws1/
cl_se2emailaddresslist_w=>tt_emailaddresslist.
    APPEND NEW /aws1/cl_se2emailaddresslist_w( iv_value =
iv_to_email_address ) TO lt_to_addresses.
    DATA(lo_destination) = NEW /aws1/cl_se2destination(
        it_toaddresses = lt_to_addresses ).

    " Create template reference
    DATA(lo_template) = NEW /aws1/cl_se2template(
        iv_templatename = iv_template_name
        iv_templatedata = iv_template_data ).

    DATA(lo_content) = NEW /aws1/cl_se2emailcontent(
        io_template = lo_template ).

    " Create list management options
    DATA(lo_list_mgmt) = NEW /aws1/cl_se2listmanagementopts(
        iv_contactlistname = iv_contact_list_name ).

    " Send the email using template
    lo_se2->sendemail(
        iv_fromemailaddress = iv_from_email_address
        io_destination = lo_destination
        io_content = lo_content
        io_listmanagementoptions = lo_list_mgmt ).
    MESSAGE 'Email sent using template successfully.' TYPE 'I'.
    CATCH /aws1/cx_se2accountsuspendedex INTO DATA(lo_account_suspended).
        MESSAGE 'Account suspended.' TYPE 'I'.
        RAISE EXCEPTION lo_account_suspended.

```



```
CATCH /aws1/cx_se2badrequestex INTO DATA(lo_bad_request).  
  MESSAGE 'Bad request.' TYPE 'I'.  
  RAISE EXCEPTION lo_bad_request.  
CATCH /aws1/cx_se2messagerejected INTO DATA(lo_message_rejected).  
  MESSAGE 'Message rejected - check email verification.' TYPE 'I'.  
  RAISE EXCEPTION lo_message_rejected.  
ENDTRY.
```

- Pour plus de détails sur l'API, consultez [SendEmail](#) la section de référence du AWS SDK pour l'API SAP ABAP.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Scénarios d'utilisation de l'API Amazon SES v2 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 dans l'API Amazon SES v2 ou en les combinant avec d'autres Services AWS. Chaque exemple inclut un lien vers le code source complet, où vous trouverez des instructions sur la configuration et l'exécution du code.

Les scénarios ciblent un niveau d'expérience intermédiaire pour vous aider à comprendre les actions de service dans leur contexte.

Exemples

- [Envoyer des e-mails avec des pièces jointes à l'aide de l'API Amazon SES v2](#)
- [Un scénario complet de newsletter Amazon SES API v2 utilisant un AWS Kit SDK](#)

Envoyer des e-mails avec des pièces jointes à l'aide de l'API Amazon SES v2

L'exemple de code suivant montre comment envoyer des e-mails avec des pièces jointes à l'aide de l'API Amazon SES v2.

- Créez un modèle d'e-mail pour les envois groupés.
- Envoyez un simple e-mail avec une pièce jointe.

- Envoyez un simple e-mail avec une image en ligne.
- Envoyez des modèles d'e-mails en masse avec des pièces jointes.
- nettoyer les ressources.

Python

Kit SDK for 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](#).

Exécutez un scénario interactif illustrant les pièces jointes à un e-mail.

```
class SESv2EmailAttachmentsScenario:
    """
    Demonstrates sending emails with attachments using Amazon SESv2.

    This scenario demonstrates:
    1. Setting up an email identity and template.
    2. Sending a simple email with a file attachment.
    3. Sending a simple email with an inline image.
    4. Sending bulk templated emails with attachments.
    5. Cleaning up created resources.
    """

    TEMPLATE_NAME = "AttachmentDemoTemplate"

    def __init__(self, sesv2_wrapper: SESv2Wrapper) -> None:
        """
        :param sesv2_wrapper: An instance of the SESv2Wrapper class.
        """
        self.sesv2_wrapper = sesv2_wrapper
        self.sender_email = ""
        self.recipient_emails: list = []
        self.identity_was_created = False

    def run_scenario(self) -> None:
        """Runs the SESv2 email attachments scenario."""
```

```

print("-" * 88)
print("Welcome to the Amazon SESv2 Email Attachments Scenario.")
print("-" * 88)
print(
    "This scenario demonstrates how to send emails with attachments\n"
    "using SESv2 attachment support. SES handles MIME\n"
    "construction automatically, so you don't need to build raw\n"
    "MIME messages.\n"
)

try:
    self._setup()
    self._step1_send_email_with_attachment()
    self._step2_send_email_with_inline_image()
    self._step3_send_bulk_email_with_attachments()
except Exception as e:
    logger.error("Scenario failed: %s", e)
    print(f"\nThe scenario encountered an error: {e}")
finally:
    self._cleanup()

# ----- Setup -----

def _setup(self) -> None:
    """
    Prompts for configuration, verifies the sender identity, prepares a
    sample attachment, and creates an email template.
    """
    print("\n--- Setup ---\n")

    # Prompt for sender and recipient addresses.
    print(
        "Both sender and recipient addresses must be verified if your\n"
        "account is in the SES sandbox.\n"
    )
    self.sender_email = q.ask(
        "Enter a verified sender email address: "
    )
    recipient_input = q.ask(
        "Enter one or more recipient email addresses (comma-separated): "
    )
    self.recipient_emails = [
        addr.strip() for addr in recipient_input.split(",") if addr.strip()
    ]

```

```
# Verify the sender identity.
print(f"\nChecking identity for {self.sender_email}...")
try:
    identity_info = self.sesv2_wrapper.get_email_identity(
        self.sender_email
    )
    verified = identity_info.get("VerifiedForSendingStatus", False)
    if verified:
        print(f" {self.sender_email} is verified and ready to send.")
    else:
        print(
            f" {self.sender_email} exists but is not yet verified."
        )
except ClientError as err:
    if err.response["Error"]["Code"] == "NotFoundException":
        print(
            f" Identity {self.sender_email} not found. "
            "Creating it now..."
        )
        result = self.sesv2_wrapper.create_email_identity(
            self.sender_email
        )
        self.identity_was_created = True
        print(
            f" Identity created. Verification status: "
            f"{result.get('VerifiedForSendingStatus', False)}"
        )
        print(
            " Check your inbox and click the verification link "
            "before continuing."
        )
        q.ask("Press Enter when you have verified the address...")
    else:
        raise

# Create the email template for the bulk-send step.
print("\nCreating email template for the bulk email step...")
try:
    self.sesv2_wrapper.create_email_template(
        template_name=self.TEMPLATE_NAME,
        subject="Bulk Email with Attachment for {{name}}",
        html_body=(
            "<h1>Hello {{name}}</h1>"
        )
    )
```

```

        "<p>Please find the attached document.</p>"
    ),
    text_body=(
        "Hello {{name}}, Please find the attached document."
    ),
)
print(f"  Template '{self.TEMPLATE_NAME}' created.\n")
except ClientError as err:
    if err.response["Error"]["Code"] == "AlreadyExistsException":
        print(
            f"  Template '{self.TEMPLATE_NAME}' already exists. "
            "Using it.\n"
        )
    else:
        raise

# ----- Step 1: Simple email with file attachment -----

def _step1_send_email_with_attachment(self) -> None:
    """Sends a simple email with a text file attachment."""
    print("\n--- Step 1: Send a Simple Email with a File Attachment ---\n")
    print(
        "Creating a sample text file attachment and sending it with\n"
        "the Simple email content type. SES constructs the MIME message\n"
        "automatically.\n"
    )

    # Prepare a sample text file as bytes.
    sample_content = b"This is a sample report attachment."

    attachment = {
        "RawContent": sample_content,
        "FileName": "sample-report.txt",
        "ContentType": "text/plain",
        "ContentDisposition": "ATTACHMENT",
        "ContentDescription": "Sample report text file",
        "ContentTransferEncoding": "BASE64",
    }

    print(
        "Note: When using an AWS SDK, the SDK handles base64 encoding\n"
        "automatically. Direct API callers must encode content themselves.\n"
    )

```

```

message_id = self.sesv2_wrapper.send_email(
    from_address=self.sender_email,
    to_addresses=self.recipient_emails,
    subject="SESV2 Attachment Demo - Simple Email with Attachment",
    html_body=(
        "<h1>Attachment Demo</h1>"
        "<p>Please see the attached <b>report document</b>.</p>"
    ),
    text_body="Please see the attached report document.",
    attachments=[attachment],
)

print(f" Email sent. MessageId: {message_id}")
print(
    " SES automatically constructed the MIME message with the "
    "attachment.\n"
)

# ----- Step 2: Simple email with inline image -----

def _step2_send_email_with_inline_image(self) -> None:
    """Sends a simple email with an inline image that renders in HTML."""
    print("\n--- Step 2: Send a Simple Email with an Inline Image ---\n")
    print(
        "This step demonstrates INLINE disposition. The image renders\n"
        "directly in the HTML body using a 'cid:' reference instead of\n"
        "appearing as a downloadable attachment.\n"
    )

    # Create a minimal 1x1 red PNG (valid PNG file).
    sample_image = (
        b"\x89PNG\r\n\x1a\n" # PNG signature
        b"\x00\x00\x00\rIHDR\x00\x00\x00\x01\x00\x00\x00\x01"
        b"\x08\x02\x00\x00\x00\x90wS\xde" # 1x1 RGB
        b"\x00\x00\x00\x0cIDATx\x9cc\xf8\x0f\x00\x00\x01\x01"
        b"\x00\x05\x18\xd8N" # compressed data
        b"\x00\x00\x00\x00IEND\xaeB`x82" # IEND
    )

    attachment = {
        "RawContent": sample_image,
        "FileName": "logo.png",
        "ContentType": "image/png",
        "ContentDisposition": "INLINE",
    }

```

```

        "ContentId": "logo123",
        "ContentDescription": "Company logo",
        "ContentTransferEncoding": "BASE64",
    }

    html_body = (
        "<html><body>"
        "<h1>Inline Image Demo</h1>"
        "<p>Here is our logo:</p>"
        ''
        "</body></html>"
    )

    message_id = self.sesv2_wrapper.send_email(
        from_address=self.sender_email,
        to_addresses=self.recipient_emails,
        subject="SESV2 Attachment Demo - Inline Image",
        html_body=html_body,
        text_body=(
            "Inline Image Demo - Please view this email in an "
            "HTML-capable client to see the embedded image."
        ),
        attachments=[attachment],
    )

    print(f" Email sent. MessageId: {message_id}")
    print(
        " The ContentId 'logo123' is referenced in the HTML body via\n"
        " 'cid:logo123', which lets the image render inline.\n"
    )

# ----- Step 3: Bulk templated email with attachments -----

def _step3_send_bulk_email_with_attachments(self) -> None:
    """Sends bulk templated emails with attachments to multiple
    recipients."""
    print("\n--- Step 3: Send Bulk Templated Emails with Attachments ---\n")
    print(
        "Using SendBulkEmail to send a templated email with an attachment\n"
        "to multiple recipients in a single API call. Each recipient gets\n"
        "personalized content via template data.\n"
    )

    sample_content = b"This is a sample report attachment."

```

```

attachment = {
    "RawContent": sample_content,
    "FileName": "sample-report.txt",
    "ContentType": "text/plain",
    "ContentDisposition": "ATTACHMENT",
    "ContentDescription": "Sample report for bulk recipients",
    "ContentTransferEncoding": "BASE64",
}

# Build one entry per recipient with personalized names.
names = ["Alice", "Bob", "Charlie", "Diana", "Eve"]
bulk_entries = []
for i, email in enumerate(self.recipient_emails):
    name = names[i] if i < len(names) else f"Recipient{i + 1}"
    bulk_entries.append(
        {
            "Destination": {"ToAddresses": [email]},
            "ReplacementEmailContent": {
                "ReplacementTemplate": {
                    "ReplacementTemplateData": json.dumps(
                        {"name": name}
                    )
                }
            },
        },
    )

results = self.sesv2_wrapper.send_bulk_email(
    from_address=self.sender_email,
    template_name=self.TEMPLATE_NAME,
    default_template_data='{"name": "Valued Customer"}',
    bulk_entries=bulk_entries,
    attachments=[attachment],
)

print(" Bulk email results:")
for idx, result in enumerate(results):
    status = result.get("Status", "Unknown")
    msg_id = result.get("MessageId", "N/A")
    error = result.get("Error", "")
    recipient = (
        self.recipient_emails[idx]
        if idx < len(self.recipient_emails)

```



```

        else "Unknown"
    )
    print(f"    {recipient}: Status={status}, MessageId={msg_id}")
    if error:
        print(f"        Error: {error}")

    print(
        "\n All recipients receive the same attachment(s) defined in\n"
        " DefaultContent. Template data is personalized per recipient.\n"
    )

# ----- Cleanup -----

def _cleanup(self) -> None:
    """Deletes the email template and optionally the email identity."""
    print("\n--- Cleanup ---\n")

    # Delete the email template.
    try:
        self.sesv2_wrapper.delete_email_template(self.TEMPLATE_NAME)
        print(f" Template '{self.TEMPLATE_NAME}' deleted.")
    except ClientError as err:
        if err.response["Error"]["Code"] == "NotFoundException":
            print(
                f" Template '{self.TEMPLATE_NAME}' was already deleted."
            )
        else:
            logger.error("Failed to delete template: %s", err)

    # Optionally delete the email identity.
    if self.identity_was_created and self.sender_email:
        delete_identity = q.ask(
            f"Delete the email identity '{self.sender_email}'? (y/n) ",
            q.is_yn,
        )
        if delete_identity:
            try:
                self.sesv2_wrapper.delete_email_identity(
                    self.sender_email
                )
                print(
                    f" Email identity '{self.sender_email}' deleted."
                )
            except ClientError as err:

```

```

        if err.response["Error"]["Code"] == "NotFoundException":
            print(
                f" Identity '{self.sender_email}' was "
                "already deleted."
            )
        else:
            logger.error(
                "Failed to delete identity: %s", err
            )
    else:
        print(
            f" Skipping identity deletion for {self.sender_email}."
        )
    else:
        print(
            " Sender identity was pre-existing. Skipping deletion."
        )

    print("\nAll resources have been cleaned up.")
    print("-" * 88)

```

Créez une classe wrapper SESv2 pour gérer les opérations.

```

class SESv2Wrapper:
    """Encapsulates Amazon SESv2 email sending actions."""

    def __init__(self, sesv2_client: Any) -> None:
        """
        Initializes the SESv2Wrapper with an SESv2 client.

        :param sesv2_client: A Boto3 SESv2 client.
        """
        self.sesv2_client = sesv2_client

    @classmethod
    def from_client(cls) -> "SESv2Wrapper":
        """
        Creates an SESv2Wrapper instance with a default Boto3 SESv2 client.

        :return: A new SESv2Wrapper instance.

```

```

    """
    sesv2_client = boto3.client("sesv2")
    return cls(sesv2_client)

def get_email_identity(self, email_address: str) -> Dict[str, Any]:
    """
    Gets information about an email identity, including its verification
    status.

    :param email_address: The email address or domain to look up.
    :return: A dictionary with identity information including verification
    status.
    :raises ClientError: If the identity is not found (NotFoundException).
    """
    try:
        response = self.sesv2_client.get_email_identity(
            EmailIdentity=email_address
        )
        logger.info("Got email identity for %s.", email_address)
        return response
    except ClientError as err:
        if err.response["Error"]["Code"] == "NotFoundException":
            logger.info(
                "Email identity %s not found.", email_address
            )
        else:
            logger.error(
                "Couldn't get email identity %s. Here's why: %s: %s",
                email_address,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
        raise

def create_email_identity(self, email_address: str) -> Dict[str, Any]:
    """
    Starts the process of verifying an email identity (email address or
    domain).

    :param email_address: The email address or domain to verify.
    :return: A dictionary with the identity type and verification status.
    :raises ClientError: If the limit is exceeded (LimitExceededException).

```

```

    """
    try:
        response = self.sesv2_client.create_email_identity(
            EmailIdentity=email_address
        )
        logger.info(
            "Started verification for email identity %s.", email_address
        )
        return response
    except ClientError as err:
        if err.response["Error"]["Code"] == "LimitExceededException":
            logger.error(
                "Couldn't create email identity %s. You have exceeded "
                "the maximum number of email identities. "
                "Use an existing verified identity.",
                email_address,
            )
        else:
            logger.error(
                "Couldn't create email identity %s. Here's why: %s: %s",
                email_address,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
        raise

def create_email_template(
    self,
    template_name: str,
    subject: str,
    html_body: str,
    text_body: str,
) -> None:
    """
    Creates an email template for use with templated and bulk email sends.

    :param template_name: The name for the new template.
    :param subject: The subject line of the template. May include
    {{placeholders}}.
    :param html_body: The HTML body of the template.
    :param text_body: The plain text body of the template.
    :raises ClientError: If the template limit is exceeded
    (LimitExceededException).

```

```

    """
    try:
        self.sesv2_client.create_email_template(
            TemplateName=template_name,
            TemplateContent={
                "Subject": subject,
                "Html": html_body,
                "Text": text_body,
            },
        )
        logger.info("Created email template %s.", template_name)
    except ClientError as err:
        if err.response["Error"]["Code"] == "LimitExceededException":
            logger.error(
                "Couldn't create email template %s. You have exceeded "
                "the maximum number of email templates. "
                "Delete unused templates first.",
                template_name,
            )
        else:
            logger.error(
                "Couldn't create email template %s. Here's why: %s: %s",
                template_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
        raise

def send_email(
    self,
    from_address: str,
    to_addresses: List[str],
    subject: str,
    html_body: str,
    text_body: str,
    attachments: Optional[List[Dict[str, Any]]] = None,
) -> str:
    """
    Sends a simple email message with optional attachments.

    SES handles MIME construction automatically when using attachments
    with the Simple content type, so developers don't need to build
    raw MIME messages.

```

```

:param from_address: The verified sender email address.
:param to_addresses: A list of recipient email addresses.
:param subject: The subject line of the email.
:param html_body: The HTML body content.
:param text_body: The plain text body content.
:param attachments: An optional list of attachment dictionaries. Each
    attachment should contain 'RawContent' (bytes), 'FileName' (str),
    and optionally 'ContentType', 'ContentDisposition', 'ContentId',
    'ContentDescription', and 'ContentTransferEncoding'.
:return: The MessageId of the sent email.
:raises ClientError: If the message is rejected (MessageRejected).
"""
try:
    simple_message: Dict[str, Any] = {
        "Subject": {"Data": subject},
        "Body": {
            "Html": {"Data": html_body},
            "Text": {"Data": text_body},
        },
    }

    if attachments:
        simple_message["Attachments"] = attachments

    response = self.sesv2_client.send_email(
        FromEmailAddress=from_address,
        Destination={"ToAddresses": to_addresses},
        Content={"Simple": simple_message},
    )
    message_id = response["MessageId"]
    logger.info(
        "Sent email from %s to %s. MessageId: %s",
        from_address,
        to_addresses,
        message_id,
    )
    return message_id
except ClientError as err:
    if err.response["Error"]["Code"] == "MessageRejected":
        logger.error(
            "Message was rejected. Check that attachments use "
            "supported file types and total message size is "
            "under 40 MB. Details: %s",

```

```

        err.response["Error"]["Message"],
    )
else:
    logger.error(
        "Couldn't send email. Here's why: %s: %s",
        err.response["Error"]["Code"],
        err.response["Error"]["Message"],
    )
raise

def send_bulk_email(
    self,
    from_address: str,
    template_name: str,
    default_template_data: str,
    bulk_entries: List[Dict[str, Any]],
    attachments: Optional[List[Dict[str, Any]]] = None,
) -> List[Dict[str, Any]]:
    """
    Sends a templated email to multiple recipients in a single API call.

    All recipients receive the same attachment(s) defined in the default
    content, while template data can be personalized per recipient.

    :param from_address: The verified sender email address.
    :param template_name: The name of an existing email template.
    :param default_template_data: Default JSON template data string.
    :param bulk_entries: A list of BulkEmailEntry dicts, each containing
        'Destination' and optionally 'ReplacementEmailContent'.
    :param attachments: An optional list of attachment dicts for all
        recipients.
    :return: A list of BulkEmailEntryResult dicts with status and MessageId.
    :raises ClientError: If the message is rejected (MessageRejected).
    """
    try:
        template_content: Dict[str, Any] = {
            "TemplateName": template_name,
            "TemplateData": default_template_data,
        }

        if attachments:
            template_content["Attachments"] = attachments

```

```

        response = self.sesv2_client.send_bulk_email(
            FromEmailAddress=from_address,
            DefaultContent={"Template": template_content},
            BulkEmailEntries=bulk_entries,
        )
    results = response.get("BulkEmailEntryResults", [])
    logger.info(
        "Sent bulk email from %s to %d recipients.",
        from_address,
        len(bulk_entries),
    )
    return results
except ClientError as err:
    if err.response["Error"]["Code"] == "MessageRejected":
        logger.error(
            "Bulk message was rejected. Check that the template "
            "exists, attachment file types are supported, and "
            "total message size is within limits. Details: %s",
            err.response["Error"]["Message"],
        )
    else:
        logger.error(
            "Couldn't send bulk email. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
    raise

def delete_email_template(self, template_name: str) -> None:
    """
    Deletes an email template.

    :param template_name: The name of the template to delete.
    :raises ClientError: If the template is not found (NotFoundException).
    """
    try:
        self.sesv2_client.delete_email_template(
            TemplateName=template_name
        )
        logger.info("Deleted email template %s.", template_name)
    except ClientError as err:
        if err.response["Error"]["Code"] == "NotFoundException":
            logger.info(

```



```

        "Email template %s not found or already deleted.",
        template_name,
    )
else:
    logger.error(
        "Couldn't delete email template %s. Here's why: %s: %s",
        template_name,
        err.response["Error"]["Code"],
        err.response["Error"]["Message"],
    )
    raise

def delete_email_identity(self, email_address: str) -> None:
    """
    Deletes an email identity.

    :param email_address: The email address or domain to delete.
    :raises ClientError: If the identity is not found (NotFoundException).
    """
    try:
        self.sesv2_client.delete_email_identity(
            EmailIdentity=email_address
        )
        logger.info("Deleted email identity %s.", email_address)
    except ClientError as err:
        if err.response["Error"]["Code"] == "NotFoundException":
            logger.info(
                "Email identity %s not found or already deleted.",
                email_address,
            )
        else:
            logger.error(
                "Couldn't delete email identity %s. Here's why: %s: %s",
                email_address,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise

```

- Pour plus de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK for Python (Boto3).
 - [CreateEmailIdentity](#)
 - [CreateEmailTemplate](#)
 - [DeleteEmailIdentity](#)
 - [DeleteEmailTemplate](#)
 - [GetEmailIdentity](#)
 - [SendBulkEmail](#)
 - [SendEmail](#)

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit SDK.

Un scénario complet de newsletter Amazon SES API v2 utilisant un AWS Kit SDK

Les exemples de code suivants montrent comment exécuter le scénario de newsletter de l'API Amazon SES v2.

.NET

SDK pour .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](#).

Exécutez le scénario.

```
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 scenario demonstrates how to use the Amazon Simple Email Service (SES)
        v2 to send a coupon newsletter to a list of subscribers.
        The scenario 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 resources folder.
private static string _resourcesFilePathLocation = "../..../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
Scenario.");
        Console.WriteLine("This scenario 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 scenario 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 scenario.
/// </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.WriteLine("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.WriteLine("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 scenario.
    /// </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);
    }
}

```

Encapsuleur 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 de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK pour .NET .
 - [CreateContact](#)
 - [CreateContactList](#)
 - [CreateEmailIdentity](#)
 - [CreateEmailTemplate](#)
 - [DeleteContactList](#)
 - [DeleteEmailIdentity](#)
 - [DeleteEmailTemplate](#)
 - [ListContacts](#)
 - [SendEmail.simple](#)
 - [SendEmail.template](#)

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](#).

```
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 de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK for Java 2.x .
 - [CreateContact](#)
 - [CreateContactList](#)
 - [CreateEmailIdentity](#)
 - [CreateEmailTemplate](#)
 - [DeleteContactList](#)
 - [DeleteEmailIdentity](#)
 - [DeleteEmailTemplate](#)
 - [ListContacts](#)
 - [SendEmail.simple](#)
 - [SendEmail.template](#)

Python

Kit SDK for 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](#).

```
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

    def try_create_contact_list_and_send_email(self, email):
        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.template](#)

Rust

SDK pour Rust

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](#).

```
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 de détails sur l'API, consultez les rubriques suivantes dans la Référence des API du kit AWS SDK pour Rust.
 - [CreateContact](#)
 - [CreateContactList](#)
 - [CreateEmailIdentity](#)
 - [CreateEmailTemplate](#)
 - [DeleteContactList](#)
 - [DeleteEmailIdentity](#)
 - [DeleteEmailTemplate](#)
 - [ListContacts](#)
 - [SendEmail.simple](#)
 - [SendEmail.template](#)

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultez [Utilisation d'Amazon SES avec un AWS Kit SDK](#). Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit 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.

- [Protection des données dans Amazon Simple Email Service](#)
- [Gestion des identités et des accès dans Amazon SES](#)
- [Journalisation et surveillance dans Amazon SES](#)
- [Validation de la conformité pour Amazon Simple Email Service](#)
- [Amazon Simple Email Service](#)
- [Sécurité de l'infrastructure dans Amazon Simple Email Service](#)
- [Configuration des points de terminaison d'un VPC avec Amazon SES](#)

Protection des données dans Amazon Simple Email Service

Le modèle de [responsabilité AWS partagée \(modèle\)](#) 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 la [FAQ sur la confidentialité des données](#) et les . Pour plus d'informations sur la protection des données en Europe, consultez le [Centre du règlement général sur la protection des données \(RGPD\)](#).

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 Gestion des identités et des accès AWS (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.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section [Utilisation des CloudTrail sentiers](#) dans le guide de AWS CloudTrail l'utilisateur.
- 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 140-3 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 disponibles, consultez [Norme FIPS \(Federal Information Processing Standard\) 140-3](#).

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 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](#)
- [Chiffrement en transit](#)
- [Suppression de données personnelles d'Amazon SES](#)

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 .

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](#) dans le Guide du développeur AWS Key Management Service .

Note

Pour l'archivage, votre clé doit répondre aux exigences suivantes :

- La clé doit être symétrique.
- L'origine du matériau clé doit être `AWS_KMS`.
- La clé d'utilisation doit être `ENCRYPT_DECRYPT`.

Stratégie de clé

Les stratégies de clé 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 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 Mail Manager

Vous pouvez spécifier une clé gérée par le client au lieu d'utiliser des clés AWS détenues. Lorsque vous créez une archive ou configurez un point de terminaison d'entrée avec une authentification TLS mutuelle (mTLS), vous pouvez spécifier la clé de données en saisissant un ARN de clé KMS. Pour l'archivage, Mail Manager utilise la clé pour chiffrer toutes les données client contenues dans l'archive. Pour les points de terminaison d'entrée MTL, Mail Manager utilise la clé pour chiffrer le contenu du trust store au repos.

- 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 politiques [Politiques 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).

Exemple

```
"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.

Exemple

Vous trouverez ci-dessous des exemples d'instructions 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 instruction 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": "*"
},

```

Politiques MTL relatives aux terminaux d'entrée

Les exemples de politiques suivants permettent d'utiliser une clé gérée par le client pour chiffrer le contenu du trust store pour l'authentification TLS mutuelle (MTLS) sur les points de terminaison d'entrée de Mail Manager.

Pour appliquer les exemples de politiques à un point de terminaison d'entrée spécifique, remplacez le caractère générique de la condition par un ARN de ressource exact (par exemple, `arn:aws:ses:us-east-1:111122223333:mailmanager-ingress-point/inp-ab1c2defgh3ij4klmno5pq6rs`).

Politique IAM

```

{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/rolename"
  },

```

```

    "Action": [
      "kms:GenerateDataKey",
      "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "kms:ViaService": "ses.us-east-1.amazonaws.com"
      },
      "StringLike": {
        "kms:EncryptionContext:aws:ses:arn": [
          "arn:aws:ses:us-east-1:111122223333:mailmanager-ingress-point/*"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/rolename"
    },
    "Action": [
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "kms:ViaService": "ses.us-east-1.amazonaws.com"
      }
    }
  }
}

```

AWS KMS stratégie

```

{
  "Effect": "Allow",
  "Principal": {
    "Service": "ses.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt"
  ],
  "Resource": "*",

```

```

    "Condition": {
      "StringLike": {
        "aws:SourceArn": [
          "arn:aws:ses:us-east-1:111122223333:mailmanager-ingress-point/*"
        ],
        "kms:EncryptionContext:aws:ses:arn": [
          "arn:aws:ses:us-east-1:111122223333:mailmanager-ingress-point/*"
        ]
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ses.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "aws:SourceArn": [
            "arn:aws:ses:us-east-1:111122223333:mailmanager-ingress-point/*"
          ]
        }
      }
    }
  ]
}

```

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": "57f5dbec-16da-413e-979f-2c4c6663475e"  
}
```

Decrypt

Lorsque vous accédez à une ressource cryptée, SES appelle l'opération Decrypt 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": "AROAIQDTESTANDEXAMPLE:Sampleuser01",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE: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 de plus amples informations, veuillez consulter [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](#)
- [Supprimer des données relatives à des e-mails envoyés à l'aide d'Amazon SES](#)
- [Supprimer des données relatives aux identités](#)
- [Supprimer des données d'authentification d'expéditeur](#)
- [Supprimer des données relatives aux règles de réception](#)
- [Supprimer des données relatives à des filtres d'adresses IP](#)
- [Supprimer des données dans les modèles d'e-mail](#)
- [Supprimer des données dans des modèles d'e-mail de vérification personnalisé](#)
- [Supprimer toutes les données personnelles en fermant votre AWS compte](#)

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 en utilisant 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 contiennent 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 SES 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 par 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 de AWS IDs (qui sont associées 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 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 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 qui contient la politique d'authentification de l'expéditeur. Remplacez *samplePolicy* par le nom de la politique d'authentification de l'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 de l'ensemble 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'adresse 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 votre AWS compte 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 Gestion des identités et des accès AWS (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.
- Pour contrôler les aspects généraux de l'utilisation des API, tels que la période pendant laquelle un utilisateur est autorisé à appeler l'API APIs qu'il est autorisé 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'**Action**élément permet uniquement l'accès à l'envoi d'e-mails APIs (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 `Resource` à envoyer, définissez ARNs les identités que vous autorisez l'utilisateur à utiliser.

Si l'**Action**élément permet d'accéder à tous APIs :

- 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 autorisations non-email-sending APIs et `Resource` défini sur `*`
 - L'un étant `Action` défini sur l'un des envois d'e-mails APIs (`ses:SendEmail` et/ou `ses:SendRawEmail`) et `Resource` défini sur le 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 APIs informations indiquées dans le tableau suivant.

Clé de condition	Description	API
<code>ses:Recipients</code>	Restreint les adresses des destinataires, qui incluent les adresses « To: », « CC » et « BCC ».	<code>SendEmail</code> , <code>SendRawEmail</code>
<code>ses:FromAddress</code>	Limite l'adresse d'expédition.	<code>SendEmail</code> , <code>SendRawEmail</code> , <code>SendBounce</code>
<code>ses:FromDisplayName</code>	Limite l'adresse d'expédition utilisée comme nom d'affichage.	<code>SendEmail</code> , <code>SendRawEmail</code>
<code>ses:FeedbackAddress</code>	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.	<code>SendEmail</code> , <code>SendRawEmail</code>

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 .	
<code>ses:MultiRegionEndpointId</code>	Vous permet de contrôler quel identifiant de point de terminaison est utilisé lors de l'envoi d'e-mails	<code>SendEmail</code> , <code>SendBulkEmail</code>

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 APIs. 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.

JSON

```
{
  "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.

JSON

```
{
    "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.

JSON

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

```

```
    "Resource": "*"
  }
]
}
```

Restriction de la période d'envoi

La politique suivante permet à un utilisateur d'appeler SES pour envoyer des e-mails APIs uniquement pendant le mois de septembre 2018.

JSON

```
{
  "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 politique suivante permet à un utilisateur d'appeler le SES pour envoyer des e-mails APIs, mais uniquement aux adresses des destinataires du domaine example.com (en distinguant majuscules et StringLike minuscules).

JSON

```
{
  "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 politique suivante permet à un utilisateur d'appeler le service d'envoi d'e-mails de SES APIs, mais uniquement si l'adresse « De » est marketing@example.com.

JSON

```
{
  "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'[SendBounce](#) API, mais uniquement si l'adresse « De » est bounce@example.com.

JSON

```
{
  "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 politique suivante permet à un utilisateur d'appeler le service d'envoi d'e-mails de SES APIs, mais uniquement si le nom d'affichage de l'adresse « De » inclut le service Marketing (StringLike en distinguant majuscules et minuscules).

JSON

```
{
  "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 politique suivante permet à un utilisateur d'appeler le service d'envoi d'e-mails SES APIs, mais uniquement si le « chemin de retour » de l'e-mail est défini sur `feedback@example.com`.

JSON

```
{
  "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 : Amazon SESFull Access

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 [Amazon SESFull Access](#) dans le manuel AWS Managed Policy Reference.

AWS politique gérée : Amazon SESRead OnlyAccess

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 [Amazon SESRead OnlyAccess](#) dans le AWS Managed Policy Reference.

AWS politique gérée : Amazon SESService RolePolicy

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 de plus amples informations, veuillez consulter [Autorisations de rôle liées à un service pour Amazon SES](#).

Pour consulter les autorisations associées à cette politique, consultez [Amazon SESService RolePolicy](#) dans le 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.

Modifier	Description	Date
Amazon Simple Email Service a ajouté une nouvelle politique gérée	Amazon Simple Email Service a été ajouté AmazonSES ServiceRolePolicy au rôle lié au service AWSServiceRoleForAmazonSES qui permet à SES d'effectuer des actions en votre nom	13 mai 2024
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	30 avril 2024

Modifier	Description	Date
	suivante : Amazon Simple Email Service a été ajouté ses :BatchGetMetricData à la politique SESReadOnlyAccess gérée par Amazon. Cela donnera accès à l'API SES BatchGetMetricData	
Amazon Simple Email Service a mis à jour une définition de politique	Amazon Simple Email Service a été ajouté ses :BatchGet* à la politique SESReadOnlyAccess gérée par Amazon. Cela donnera accès à l'API SES BatchGetMetricData	16 févr. 2024
Amazon Simple Email Service a modifié deux définitions de politique	Amazon Simple Email Service a été supprimé « via la console de AWS gestion » à la fin des SESReadOnlyAccess définitions Amazon SESFullAccess et Amazon	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) Gestion des identités et des accès AWS 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 de confiance 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 qui prennent en charge les rôles liés à un service, consultez la section [AWS Services qui fonctionnent avec IAM](#) et recherchez les services dont la valeur est Oui dans la colonne 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`. Il permet à SES de publier les mesures de surveillance CloudWatch de base d'Amazon pour le compte de vos ressources SES.

Le rôle lié au service `AWSService RoleForAmazon SES` fait confiance au service suivant pour assumer le rôle :

- `ses.amazonaws.com`

La politique d'autorisations de rôle nommée `Amazon SESService RolePolicy` 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, voir [Journalisation 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, voir [Journalisation 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, voir [Journalisation 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 lié au service AWSService RoleForAmazon SES. Après avoir 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 service AWSService RoleForAmazon SES. Pour plus d'informations, consultez la section [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 rôle AWSService RoleForAmazon SES dans les régions suivantes.

Nom de la région	Identité de la région	Support dans SES
USA Est (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 joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon SES et de vos AWS solutions. AWS fournit des outils pour vous aider à surveiller Amazon SES et à répondre aux incidents potentiels.

- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez 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 [Extraction des données d'événements Amazon SES depuis CloudWatch](#) et [Création d'alarmes de surveillance de réputation en utilisant CloudWatch](#).

- AWS CloudTrail capture les appels d'API et les événements associés effectués par vous ou en votre nom Compte AWS et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. 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 SES est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans SES. CloudTrail capture les appels d'API pour SES sous forme d'événements. Les appels capturés incluent des appels provenant de la console SES et des appels de code vers les opérations de l'API SES. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour SES. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à SES, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite et des informations supplémentaires.

Pour en savoir plus CloudTrail, notamment comment le configurer et l'activer, consultez le [guide de AWS CloudTrail l'utilisateur](#).

Informations SES dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité événementielle prise en charge se produit dans SES, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS.

Pour plus d'informations, consultez la section [Affichage des événements à l'aide de l'historique des CloudTrail événements](#).

Pour un enregistrement continu des événements survenus dans votre environnement Compte AWS, y compris des événements pour SES, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- [Vue d'ensemble de la création d'un journal d'activité](#)
- [CloudTrail Services et intégrations pris en charge](#)
- [Configuration des notifications Amazon SNS pour CloudTrail](#)
- [Réception de fichiers CloudTrail journaux de plusieurs régions](#) et [réception de fichiers CloudTrail journaux de plusieurs comptes](#)

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 faite avec les informations d'identification de l'utilisateur root ou Gestion des identités et des accès AWS (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 demande a été faite par un autre AWS service.

Pour plus d'informations, consultez la section [Élément userIdentity CloudTrail](#).

Événements liés aux données SES dans CloudTrail

[Les événements de données](#) fournissent des informations sur les opérations de ressource effectuées sur ou dans une ressource. Ils sont également connus sous le nom opérations de plans de données. Les événements de données sont souvent des activités dont le volume est élevé. Par défaut, CloudTrail n'enregistre pas les événements liés aux données. L'historique des CloudTrail événements n'enregistre pas les événements liés aux données.

Des frais supplémentaires s'appliquent pour les événements de données. Pour plus d'informations sur la CloudTrail tarification, consultez la section [AWS CloudTrail tarification](#).

 Note

L'activité d'envoi d'e-mails via l'interface SMTP de SES n'est pas enregistrée dans les CloudTrail événements. Pour un enregistrement complet des activités, utilisez le SES le plus récent APIs dans la [référence d'API SES](#) et la [référence d'API SES v2](#).

Le tableau suivant répertorie les types de ressources SES pour lesquels vous pouvez enregistrer des événements de données. La colonne Type d'événement de données (console) indique la valeur à choisir dans la liste des types d'événements de données de la CloudTrail console. La colonne de valeur `resources.type` indique la *resources.type* valeur que vous devez spécifier lors de la configuration de sélecteurs d'événements avancés à l'aide de la colonne indiquant le ou. AWS CLI CloudTrail APIs La CloudTrail colonne Données APIs enregistrées indique les appels d'API enregistrés CloudTrail pour le type de ressource.

Types de ressources SES pour les événements de données

Type d'événement de données (console)	valeur <code>resources.type</code>	Données APIs enregistrées sur CloudTrail
Identité SES	AWS: :SES : : EmailIdentity	UTILISATIONS : SendEmail SendRawEmail SendTemplatedEmail SendBulkTemplatedEmail
Kit de configuration SES	AWS: :SES : : Configura tionSet	SES version 2 : SendEmail SendBulkEmail
Modèle SES	AWS: :SES : :Modèle	UTILISATIONS :

Type d'événement de données (console)	valeur resources.type	Données APIs enregistrées sur CloudTrail
		SendTemplatedEmail
		SendBulkTemplatedEmail
		SES version 2 :
		SendEmail
		SendBulkEmail

L'exemple suivant montre comment enregistrer tous les événements de données pour toutes les identités de messagerie SES à l'aide du `--advanced-event-selectors` paramètre :

```
aws cloudtrail put-event-selectors \
--region Region \
--trail-name TrailName \
--advanced-event-selectors
'[
  {
    "Name": "Log SES data plane actions for all email identities",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::SES::EmailIdentity"] }
    ]
  }
]'
```

Vous pouvez affiner davantage les sélecteurs d'événements avancés pour filtrer les `eventName` et `resources.ARN` les champs pour n'enregistrer que les événements qui sont importants pour vous. Pour plus d'informations sur ces champs, consultez [AdvancedFieldSelector](#) dans la Référence d'API AWS CloudTrail . Pour plus d'exemples sur la façon de consigner des événements liés aux données, voir [Enregistrement des événements liés aux données](#) pour les sentiers.

CloudTrail scénarios de livraison de journaux pour la journalisation SES

CloudTrail fournit des journaux basés sur des facteurs tels que la propriété du compte et des ressources, le type d'identité et la région. La matrice suivante explique à qui et où les journaux seraient livrés en fonction de combinaisons spécifiques de ces facteurs.

Type de scénario	Rôles du compte	Ressources	Flux de demandes	Livraison de journaux
Compte croisé unique	Compte A : propriétaire de la ressource	Identité e-mail	Identité e-mail de B → A	Logs livrés à la fois à A et B
	Compte B : demandeur	E-mail de transfert de commentaires	B → E-mail de commentaires de A	Logs livrés à la fois à A et B
Plusieurs comptes croisés	Compte A : propriétaire de l'e-mail de commentaires	E-mail de commentaires (A)	C → E-mail de feedback de A +	Logs livrés à A, B et C
	Compte B : propriétaire de l'identité e-mail	Identité e-mail (B)	Identité e-mail de B	
	Compte C : demandeur			
Point de terminaison global (compte unique)	Compte A : propriétaire et demandeur	Point de terminaison global (principal : eu-west-1 et secondaire : us-west-2)	A → Point de terminaison global	Logs livrés à A dans la région qui a traité la demande (eu-west-1 ou us-west-2)
Point de terminaison global (comptes multiples)	Compte A : propriétaire de l'identité e-mail	Identité e-mail (A)	B → Identité e-mail de A via Global Endpoint	Logs livrés à A et B dans la région qui a traité la demande

Type de scénario	Rôles du compte	Ressources	Flux de demandes	Livraison de journaux
	Compte B : demandeur	Point de terminaison global (B) (eu-west-1 et us-west-2)		(eu-west-1 ou us-west-2)

Note

- CloudTrail envoie toujours les journaux sur le compte du demandeur.
- Les propriétaires des ressources reçoivent des journaux même s'ils n'ont pas effectué l'opération.
- Pour les points de terminaison mondiaux, les deux comptes nécessitent des CloudTrail abonnements dans toutes les régions configurées.
- Lors de déficiences régionales, tous les journaux apparaissent dans la région saine.

Événements de gestion de SES dans CloudTrail

SES organise des événements de gestion à CloudTrail. Les événements de gestion incluent des actions liées à la création et à la gestion de ressources au sein de 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. Pour plus d'informations sur les opérations de l'API SES, consultez la [référence des API SES et la référence des API SES v2](#).

CloudTrail entrées de fichier journal pour SES

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

Les exemples suivants illustrent CloudTrail les journaux de ces types d'événements :

Types d'événements

- [DeletelIdentity](#)
- [VerifyEmailIdentity](#)
- [SendEmail avec un contenu simple](#)
- [SendEmail avec du contenu modélisé](#)

DeletelIdentity

```
{
  "Records": [
    {
      "eventVersion": "1.11",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "ARO4D02KAWIPZEXAMPLE:myUserName",
        "arn": "arn:aws:sts::111122223333:assumed-role/users/myUserName",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "ARO4D02KAWIPZEXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/admin-role",
            "accountId": "111122223333",
            "userName": "myUserName"
          },
          "attributes": {
            "creationDate": "2025-02-27T09:53:35Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2025-02-27T09:54:31Z",
      "eventSource": "ses.amazonaws.com",
      "eventName": "DeleteIdentity",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/2.23.4",
      "requestParameters": {
```



```

        "identity": "sender@example.com"
    },
    "responseElements": null,
    "requestID": "50b87bfe-ab23-11e4-9106-5b36376f9d12",
    "eventID": "0ffa308d-1467-4259-8be3-c749753be325",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "email.us-east-1.amazonaws.com"
    }
}
]
}

```

VerifyEmailIdentity

```

{
  "Records": [
    {
      "eventVersion": "1.11",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AR0A4D02KAWIPZEXAMPLE:myUserName",
        "arn": "arn:aws:sts::111122223333:assumed-role/users/myUserName",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AR0A4D02KAWIPZEXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/admin-role",
            "accountId": "111122223333",
            "userName": "myUserName"
          },
          "attributes": {
            "creationDate": "2025-02-27T09:53:35Z",
            "mfaAuthenticated": "false"
          }
        }
      }
    }
  ]
}

```

```

    }
  },
  "eventTime": "2025-02-27T09:56:20Z",
  "eventSource": "ses.amazonaws.com",
  "eventName": "VerifyEmailIdentity",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/2.23.4",
  "requestParameters": {
    "emailAddress": "sender@example.com"
  },
  "responseElements": null,
  "requestID": "eb2ff803-ac09-11e4-8ff5-a56a3119e253",
  "eventID": "5613b0ff-d6c6-4526-9b53-a603a9231725",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "email.us-east-1.amazonaws.com"
  }
}
]
}

```

SendEmail avec un contenu simple

```

{
  "Records": [{
    "eventTime": "2025-01-24T11:43:00Z",
    "eventSource": "ses.amazonaws.com",
    "eventName": "SendEmail",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.23.4 md/awscrt#0.23.4",
    "requestParameters": {
      "destination": {
        "bccAddresses": ["HIDDEN_DUE_TO_SECURITY_REASONS"],
        "toAddresses": ["HIDDEN_DUE_TO_SECURITY_REASONS"],
        "ccAddresses": ["HIDDEN_DUE_TO_SECURITY_REASONS"]
      }
    }
  }]
}

```

```

    },
    "message": {
      "subject": {
        "charset": "UTF-8",
        "data": "HIDDEN_DUE_TO_SECURITY_REASONS"
      },
      "body": {
        "html": {
          "charset": "UTF-8",
          "data": "HIDDEN_DUE_TO_SECURITY_REASONS"
        },
        "text": {
          "charset": "UTF-8",
          "data": "HIDDEN_DUE_TO_SECURITY_REASONS"
        }
      }
    },
    "source": "sender@example.com"
  },
  "responseElements": null,
  "additionalEventData": {
    "sesMessageId": "01000100a11a11aa-00aa0a00-00a0-48a8-aaa7-
a174a83b456a-000000"
  },
  "requestID": "ab2cc803-ac09-11d7-8bb8-a56a3119e476",
  "eventID": "eb834e01-f168-435f-92c0-c36278378b6e",
  "readOnly": true,
  "resources": [{
    "accountId": "111122223333",
    "type": "AWS::SES::EmailIdentity",
    "ARN": "arn:aws:ses:us-east-1:111122223333:identity/sender@example.com"
  }],
  "eventType": "AwsApiCall",
  "managementEvent": false,
  "recipientAccountId": "111122223333",
  "eventCategory": "Data",
  "tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "email.us-east-1.amazonaws.com"
  }
}
]

```

```
}
```

SendEmail avec du contenu modélisé

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "ARO4A4D02KAWIPZEXAMPLE:myUserName",
    "arn": "arn:aws:sts::111122223333:assumed-role/users/myUserName",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "ARO4A4D02KAWIPZEXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin-role",
        "accountId": "111122223333",
        "userName": "admin-role"
      },
      "attributes": {
        "creationDate": "2025-03-05T18:51:06Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2025-03-05T19:16:29Z",
  "eventSource": "ses.amazonaws.com",
  "eventName": "SendEmail",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/2.23.4",
  "requestParameters": {
    "fromEmailAddress": "sender@example.com",
    "destination": {
      "toAddresses": ["HIDDEN_DUE_TO_SECURITY_REASONS"],
      "bccAddresses": ["HIDDEN_DUE_TO_SECURITY_REASONS"],
      "ccAddresses": ["HIDDEN_DUE_TO_SECURITY_REASONS"]
    },
    "emailTags": [{
      "value": "test",
      "name": "campaign"
    }], {
```

```

        "value": "cli-test",
        "name": "sender"
    }],
    "replyToAddresses": ["HIDDEN_DUE_TO_SECURITY_REASONS"],
    "content": {
        "template": {
            "templateData": "HIDDEN_DUE_TO_SECURITY_REASONS",
            "templateName": "TestTemplate"
        }
    },
    "responseElements": null,
    "additionalEventData": {
        "sesMessageId": "01000100a11a11aa-00aa0a00-00a0-48a8-aaa7-
a174a83b456a-000000"
    },
    "requestID": "50b87bfe-ab23-11e4-9106-5b36376f9d12",
    "eventID": "0ffa308d-1467-4259-8be3-c749753be325",
    "readOnly": true,
    "resources": [{
        "accountId": "111122223333",
        "type": "AWS::SES::EmailIdentity",
        "ARN": "arn:aws:ses:us-east-1:111122223333:identity/sender@example.com"
    }, {
        "accountId": "111122223333",
        "type": "AWS::SES::Template",
        "ARN": "arn:aws:ses:us-east-1:111122223333:template/TestTemplate"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111122223333",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "email.us-east-1.amazonaws.com"
    }
}

```

Validation de la conformité pour Amazon Simple Email Service

Des auditeurs tiers évaluent la sécurité et la conformité d'Amazon Simple Email Service dans le cadre de plusieurs programmes de AWS conformité. Il s'agit notamment des certifications SOC, PCI, FedRAMP, HIPAA et d'autres.

Pour une liste des AWS services concernés par des programmes de conformité spécifiques, voir [AWS Services concernés par programme de conformité AWS](#). Pour des informations générales, voir Programmes de [AWS conformité Programmes AWS](#) de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir [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 [de démarrage rapide sur la sécurité et la conformité Guides](#) sur la sécurité et la conformité — Ces guides de déploiement abordent les considérations architecturales et fournissent les étapes à suivre pour déployer des environnements de base axés sur la sécurité et la conformité sur. AWS
- AWS Ressources de <https://aws.amazon.com/compliance/resources/> de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- [Évaluation des ressources à l'aide des règles](#) énoncées dans le guide du AWS Config développeur : AWS Config évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- [AWS Security Hub CSPM](#) — Ce AWS service fournit une vue complète de l'état de votre sécurité interne, AWS ce qui vous permet de vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité.

Amazon Simple Email Service

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. 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 davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section [Infrastructure AWS mondiale](#).

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 AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section [Sécurité du AWS cloud](#). Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section [Protection de l'infrastructure](#) dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés 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 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.

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.

Limitations

- SES ne prend pas en charge les points de terminaison VPC SMTP 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.

Vous pouvez également utiliser des points de terminaison VPC avec les points de terminaison d'entrée de Mail Manager pour une ingestion sécurisée et privée des e-mails au sein de votre infrastructure réseau privée. Voir [the section called “Configuration du point de terminaison VPC”](#) le chapitre Mail Manager.

Exemple de procédure de configuration de SES dans Amazon VPC

Conditions préalables

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 la section [Par défaut VPCs](#).

 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. [Amazon EC2 limitant le trafic e-mail sur le port 25 par défaut, pour les points de terminaison SMTP, vous devrez utiliser un port autre que TCP 25, tel que TCP 465, 587, 2465 ou 2587. Pour plus d'informations, consultez Restriction sur les e-mails envoyés via le port 25.](#) Pour les points de terminaison d'API, utilisez le port 443.

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. Vous devez d'abord créer un groupe de sécurité qui permet à l'instance de communiquer avec le ou les ports choisis, puis créer un point de terminaison VPC pour Amazon SES, et enfin tester la connexion au point de terminaison VPC pour vous assurer 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. Pour les points de terminaison SMTP, vous pouvez utiliser l'un des numéros de port suivants :**465**, **5872465**, ou. **2587** Pour les points de terminaison d'API, utilisez le port 443.
 - Pour Source type (Type de source), choisissez Personnalisé.
 - Pour Source, entrez la plage d'adresses IP CIDR privées ou un autre groupe IDs de sécurité contenant les ressources qui utiliseront le point de terminaison 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 PrivateLink et Lattice, sélectionnez Endpoints.
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 panneau Services, pour les points de terminaison SMTP, filtrez sur SMTP dans la barre de recherche, puis sélectionnez le bouton radio correspondant. Pour les points de terminaison d'API, filtrez les e-mails dans la barre de recherche. Vous pouvez également utiliser un point de terminaison FIPS en recherchant email-fips.
7. Dans le volet VPC, cliquez dans la barre de recherche et sélectionnez un VPC dans la zone de liste (consultez [the section called “Conditions préalables”](#)).

8. Dans le panneau Sous-réseaux, sélectionnez Zones de disponibilité et IDsous-réseau.

 Note

Amazon SES ne prend pas en charge les points de terminaison VPC SMTP dans les zones de disponibilité suivantes use1-az2 :use1-az3,,use1-az5,usw1-az2, usw2-az4apne2-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 démarrage](#) du guide de l'utilisateur Amazon EC2.

2. Envoi d'un e-mail test Pour le point de terminaison SMTP, utilisez l'interface SMTP SES. Pour le point de terminaison de l'API, utilisez la CLI ou l'API 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 [Processus de révision d'Amazon SES Sending FAQs](#).
- Pour en savoir plus sur l'impact des listes Blackhole basées sur le DNS (DNSBLs) sur vos envois avec Amazon SES, consultez [Liste DNS Blackhole \(DNSBL\) FAQs](#)

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 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 le AWS support. Explorez plutôt les différentes options d'assistance disponibles sur la page [Contactez-nous](#).

Table des matières

- [Problèmes généraux relatifs à Amazon SES](#)
- [Problèmes de vérification d'adresse e-mail et de domaine](#)
- [Résolution des problèmes liés à la fonction DKIM dans Amazon SES](#)
- [Problèmes de remise Amazon SES](#)
- [Problèmes au niveau des e-mails reçus d'Amazon SES](#)
- [Problèmes de notifications Amazon SES](#)
- [Erreurs d'envoi d'e-mails Amazon SES](#)
- [Accroissement du débit avec Amazon SES](#)
- [Problèmes SMTP Amazon SES](#)

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](#). Toute modification que vous apportez à Amazon SES (ou à d'autres AWS services) met du temps à être visible 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'événements — Lorsque vous créez ou modifiez une destination d'événement (par exemple, pour demander [à Amazon SES d'envoyer vos données d'envoi d'e-mails à un autre AWS service](#)), il peut y avoir un délai entre le moment où vous avez créé ou modifié la destination de l'événement et le moment où les événements d'envoi d'e-mails arrivent réellement 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 des [Easy DKIM](#) ou [PAR 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 le même domaine plusieurs fois : vous devrez peut-être vérifier votre domaine plusieurs fois parce que vous envoyez dans différentes régions ou parce que vous utilisez le même domaine pour envoyer depuis plusieurs AWS comptes. 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 zone Value (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 desservent votre domaine, car ce sont eux qui contiennent le plus up-to-date d'informations sur votre domaine, ce qui peut prendre du temps à se propager 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 saisissons ce qui suit :

```
nslookup -type=CNAME 4hzwn5lmznmjy12pqf2agr3uzzzzxyz_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 4hzwn5lmznmjy12pqf2agr3uzzzzxyz_amazonses.ses-example.com avec la valeur 4hzwn5lmznmjy12pqf2agr3uzzzzxyz.dkim.amazonses.com. Si le registre est correctement publié, la commande doit générer le résultat suivant :

```
4hzwn5lmznmjy12pqf2agr3uzzzzxyz_domainkey.ses-example.com canonical name =  
"4hzwn5lmznmjy12pqf2agr3uzzzzxyz.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 AWS régions, vous devez configurer le DKIM pour chaque région séparément. De même, si vous utilisez le même domaine avec plusieurs AWS comptes, 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 ISPs requête d'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.

 Note

Microsoft Enterprise Outlook sélectionne de manière aléatoire une signature DKIM pour validation tout en ignorant l'autre. Ce comportement ne semble pas être en corrélation avec l'ordre dans lequel les signatures sont organisées, ce qui rend les solutions procédurales inefficaces. SES ne peut pas arrêter de signer des e-mails avec des signatures `amazonses.com` DKIM car celles-ci sont nécessaires pour les boucles de feedback relatives aux plaintes. Microsoft a reconnu qu'il s'agissait d'un problème connu, l'attribuant à des problèmes de résolution DNS au sein de son infrastructure. Ces échecs de résolution DNS expliqueraient pourquoi la validation des signatures DKIM semble échouer de manière aléatoire, étant donné que les clés publiques sont extraites des enregistrements DNS.

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 votre correspondance avec nous, veuillez fournir toutes les adresses de destinataires pertinentes, ainsi que toute demande IDs ou message IDs renvoyé par le `SendEmail` ou les `SendRawEmail` réponses.
- Attendez de voir si le problème n'est pas en réalité un retard plutôt qu'un échec de remise permanent. Pour lutter contre les spammeurs, certains rejettent ISPs temporairement les messages entrants provenant de serveurs d'envoi 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 “Maintenance d'une bonne réputation d'expéditeur”](#) 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 le [courriel DomainKeys identifié](#) (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. Lorsque vous avez fini de créer le message MIME, vous pouvez l'envoyer à l'aide de l'[SendRawEmail](#) API ou de l'[SendMail](#) API 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 SendRawEmail solution 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 :
 - Étant donné qu'Amazon SES ne conserve aucun message personnalisé IDs que vous avez ajouté, enregistrez un mappage entre un identifiant et l'identifiant du message Amazon SES qu'Amazon SES vous renvoie lorsqu'il 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 via le transfert de commentaires par e-mail, mais vous ne savez pas à quels destinataires les notifications correspondent. Certains ISPs expurgent l'adresse e-mail du destinataire de la plainte avant de transmettre la notification de plainte 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 conserve aucun message personnalisé IDs 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 AWS SDK qui utilise un langage de programmation prenant en charge les exceptions, Amazon SES peut générer une exception. Le type d'exception varie en fonction du kit SDK et de l'erreur. Par exemple, l'exception peut être un `Amazon SES MessageRejectedException` (le nom réel peut varier en fonction du SDK) ou une AWS exception 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 AWS erreurs générales, `MalformedQueryString` comme indiqué dans la rubrique [Erreurs courantes](#) du manuel Amazon Simple Email Service API Reference.

- L'adresse e-mail n'est pas vérifiée. Les identités suivantes n'ont pas pu être vérifiées dans la 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 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 chaque expéditeur du fichier que Régions AWS 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 “Processus d'envoi d'avis FAQs”](#).

- 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 plus d'informations, consultez la section [Comment gérer une erreur « Throttling - Taux d'envoi maximal dépassé »](#) sur le blog sur la AWS messagerie et le ciblage.
- Dépassement du taux d'envoi SMTP SigV2 maximal : vous essayez d'envoyer des messages à l'aide des informations d'identification SMTP créées avant le 10 janvier 2019 ; vos informations d'identification SMTP ont été créées à l'aide d'une ancienne version de la signature. AWS 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](#).
- Erreurs de serveur et délais d'attente : dans de rares cas, une `SendRawEmail` demande `SendEmail` ou un délai d'attente peut être dépassé ou renvoyer une erreur de serveur une fois que l'e-mail a déjà été accepté pour livraison. Si votre application tente à nouveau la demande, un deuxième e-mail avec un identifiant de message différent peut être envoyé. Pour établir une corrélation fiable entre les notifications d'événements et votre logique d'envoi, utilisez des [balises de message](#) plutôt que de vous fier uniquement à l'identifiant du message.

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. Vous pouvez envisager d'héberger votre application dans un centre de données proche du point de terminaison de l'API Amazon SES, ou sur une EC2 instance Amazon située dans la même AWS région 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 des vôtres AWS . 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 \(MTU\) réseau 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 équilibres 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 SDKs implémentent [automatiquement](#) la logique de nouvelle tentative, mais ils utilisent l'interface HTTPS au lieu du 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 <i>MessageID</i>	<i>MessageID</i> est une chaîne de caractères unique qu'Amazon SES utilise 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 actuellement 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.

Description	Code de réponse	En savoir plus
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 de plus amples informations, veuillez consulter 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 de plus amples informations, veuillez consulter 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 de plus amples informations, veuillez consulter 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 de plus amples informations, veuillez consulter 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 < <i>email-address</i> > 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 < <i>email-address</i> > 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 <i>UserARN</i> is not authorized to perform ses:SendRawEmail on resource <i>IdentityARN</i>	La politique Gestion des identités et des accès AWS (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 <i>region</i> : <i>identity0</i> , <i>identity1</i> , <i>identity2</i>	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 d'eux Région AWS. 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 fréquemment posées sur Amazon SES (FAQs)

Cette section contient les réponses aux questions fréquentes liées à l'utilisation d'Amazon SES.

Cette section contient FAQs les rubriques suivantes :

- [Adresses IP dédiées \(gérées\) FAQs](#)
- [Processus de révision d'Amazon SES Sending FAQs](#)
- [Liste DNS Blackhole \(DNSBL\) FAQs](#)
- [Statistiques d'envoi d'e-mails Amazon SES FAQs](#)

Adresses IP dédiées (gérées) FAQs

Bien qu'il [Adresses IP dédiées \(gérées\)](#) propose de nombreuses fonctionnalités automatisées pour la gestion, la mise à l'échelle et le préchauffage des adresses IP dédiées, il y a eu un certain malentendu quant à l'étendue de cette automatisation et aux responsabilités de SES. Il serait faux de supposer que « géré » signifie que SES gère complètement tous les aspects liés à la réputation de propriété intellectuelle et aux problèmes de cotation. Pour clarifier ces idées fausses, nous devons souligner que même si le service automatise les aspects techniques tels que la mise à l'échelle et le préchauffage, vous restez responsable du maintien de votre réputation d'expéditeur et de la gestion des problèmes liés à la réputation, tels que l'inscription sur une liste de blocage de réputation (RBL).

Ils FAQs répondent aux idées reçues les plus courantes concernant le champ d'application de la fonctionnalité et clarifient le modèle de responsabilité partagée entre vous et SES. Ces FAQ soulignent que même si l'aspect « géré » fait référence à la gestion de l'infrastructure technique, vous devez toujours surveiller et maintenir activement votre réputation d'expéditeur, maintenir des taux de rebond bas et traiter vous-même la plupart des demandes de radiation RBL.

Q1. Puis-je demander à SES de supprimer mon adresse IP dédiée (gérée) de la liste dans un RBL ?

Si votre adresse IP dédiée (gérée) est répertoriée dans un RBL des fournisseurs de messagerie destinataires, SES n'en est pas responsable et vous devez vous-même en demander la suppression directement auprès de l'administrateur du RBL. Il est important de surveiller votre site dédié IPs (géré) en suivant à la fois les notifications de rebond et les messages de réponse SMTP pour identifier les blocages. Cette surveillance contribue à protéger votre réputation d'expéditeur d'e-mails

et vous permet de traiter rapidement tout incident RBL susceptible de survenir, garantissant ainsi une délivrabilité constante des e-mails.

Q2. Puis-je demander à SES d'attribuer une nouvelle adresse IP dédiée (gérée) pour remplacer une adresse IP actuelle répertoriée dans un RBL qui n'est pas proposé par Spamhaus ?

Non SES n'effectue pas de rotation des adresses IP dédiées. Comme vous êtes responsable de vos adresses IP dédiées, qu'elles soient gérées ou standard, vous devez déterminer pourquoi elles sont répertoriées dans le RBL et les faire retirer vous-même de la liste.

Q3. SES peut-il surveiller le taux de rebond d'une adresse IP dédiée (gérée) attribuée à mon compte et effectuer une rotation de l'adresse lorsque le taux de rebond devient élevé ?

Non SES n'effectue pas de rotation des adresses IP dédiées lorsqu'un compte enregistre un taux de rebond élevé. Lorsque vous louez une adresse IP dédiée (gérée), seul votre compte possède le droit exclusif d'envoyer des e-mails via cette adresse IP dédiée, de sorte que SES ne peut pas surveiller votre compte. Il est de [votre responsabilité de gérer votre réputation d'expéditeur](#) et les composants de votre courrier électronique, notamment de gérer les plaintes et de maintenir un [taux de rebond inférieur à 2 %](#).

Q4. Je viens de louer une adresse IP dédiée (gérée) et le courrier électronique envoyé par son intermédiaire est renvoyé parce que l'adresse se trouve sur un RBL. SES vérifie-t-il la réputation d'une adresse IP dédiée (gérée) avant de la louer à un compte ?

Oui. SES réinitialise toute adresse IP dédiée (gérée) (30 jours) avant de la louer à un compte SES. La réputation revient généralement à la plupart des principaux fournisseurs. SES veille à ce que l'adresse ne figure sur aucun RBL, comme Spamhaus ; toutefois, SES ne surveille pas toutes les adresses RBLs disponibles, notamment les plus petites ou les adresses régionales. RBLs Si vous avez des inquiétudes concernant un RBL en raison d'une orientation B2B ou d'une focalisation sur les fournisseurs régionaux utilisant ces domaines, vous devez vérifier vous-même l'état de réputation de l'adresse IP dédiée (gérée).

Q5. Si SES n'intervient pas lorsque des adresses IP dédiées (gérées) sont répertoriées dans un RBL, autre que Spamhaus, pourquoi devrais-je les utiliser ?

Les adresses IP dédiées (gérées) sont gérées en termes d'auto-scaling en ajoutant et en supprimant des adresses IP en fonction du trafic. Cela vous permet également de gagner du temps en termes de gestion du [préchauffage par FAI](#) ; ainsi, un pool géré permet de suivre le nombre d'e-mails pouvant être envoyés par chaque adresse IP en fonction de l'historique des habitudes d'envoi. Vous trouverez d'autres avantages dans [the section called “Avantages et fonctionnalités”](#).

Q6. Comment puis-je suivre les adresses IP dédiées (gérées) louées à mon compte ?

Vous pouvez utiliser un ensemble de configuration SES avec une [destination de publication d'événements](#) définie pour un sujet Amazon Data Firehose ou Amazon SNS. Les événements de livraison SES incluent le tag [ses:outgoing-ip](#). Ainsi, si un e-mail a été renvoyé en raison de la réputation d'une adresse IP dédiée (gérée), vous pouvez trouver l'adresse IP dédiée incriminée (gérée) dans le tag de l'événement de rebond. `ses:outgoing-ip`

Processus de révision d'Amazon SES Sending FAQs

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](#)
- [FAQ sur les suspensions d'envoi](#)
- [FAQ sur les retours à l'expéditeur](#)

- [FAQ sur les réclamations](#)
- [FAQ sur les pièges pour le courrier indésirable](#)
- [FAQ sur les enquêtes manuelles](#)

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 de plus amples informations, veuillez consulter [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, consultez [Création d'alarmes de surveillance de réputation en utilisant CloudWatch](#).

Vous pouvez également utiliser le [Account 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 Tableau de bord AWS Health (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 de plus amples informations, veuillez consulter [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. Divulgez-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 sur [Réception 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 de plus amples informations, veuillez consulter [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 de plus amples informations, veuillez consulter [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 le [FAQ 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 votre propre feedback personnalisé IDs (jusqu'à deux) à l'aide des balises `ses:feedback-id-a` et `ses:feedback-id-b` message, 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 des 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 de plus amples informations, veuillez consulter [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. Divulgez-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'GetSendStatistics API ?

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'GetSendStatisticsAPI 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 (voir [Configuration 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 message personnalisé IDs 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 de plus amples informations, veuillez consulter [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 du taux de plaintes que vous récupérez à l'aide de la console SES ou de l'GetSendStatisticsAPI 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 le [FAQ 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 du taux de plaintes que vous récupérez à l'aide de la console SES ou de l'GetSendStatisticsAPI 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 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. Divulgez-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 « corrigéables » ?

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.

Liste DNS Blackhole (DNSBL) FAQs

Les listes de trous noirs basées sur le système de noms de domaine (DNSBLs), parfois appelées listes de trous noirs en temps réel (RBLs), listes de refus, listes de blocage ou listes noires, sont destinées à informer les fournisseurs de messagerie des adresses IP soupçonnées d'envoyer des e-mails indésirables.

Différents DNSBLs ont des impacts différents sur la délivrabilité des e-mails. Cette rubrique décrit l'impact de la livraison des e-mails que vous envoyez à l'aide d'Amazon SES, ainsi que nos politiques de suppression des adresses IP d'Amazon SES DNSBLs.

Note

Cette rubrique concerne les outils utilisés par DNSBLs 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. Quel est l'impact des DNSBLs sur la livraison des e-mails ?

Les différences des DNSBLs ont des répercussions différentes sur la réussite de la transmission d'un message. Les principaux fournisseurs de messagerie, notamment Gmail, Hotmail, AOL et Yahoo, semblent reconnaître un très petit nombre d'e-mails très réputés DNSBLs, tels que ceux proposés par Spamhaus. D'après notre expérience, d'autres DNSBLs ont tendance à avoir un faible impact, bien que certains systèmes de messagerie mettent l'accent sur certains DNSBLs plutôt que sur 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 se retrouvent les adresses IP DNSBLs ?

Il existe plusieurs façons pour une adresse IP de se retrouver sur une liste DNSBL. Les adresses IP peuvent être ajoutées DNSBLs lorsqu'elles envoient un e-mail à un spamtrap. 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. Certains autorisent DNSBLs également les utilisateurs individuels à soumettre des adresses IP. Quelques-uns autorisent DNSBLs même les utilisateurs à soumettre des plages d'adresses IP complètes. D'autres DNSBLs sont gérés grâce aux contributions des administrateurs de messagerie et peuvent inclure des adresses IP qui, selon les administrateurs, abusent de leurs propres systèmes.

Q3. Comment Amazon SES empêche-t-il l'affichage de ses adresses IP DNSBLs ?

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. L'application de nos politiques d'envoi de cette manière contribue à réduire les risques que nos adresses IP soient transmises DNSBLs.

Q4. Est-il possible pour Amazon SES que ses adresses IP soient supprimées d'une liste DNSBL ?

En ce qui concerne SES shared IPs, nous surveillons activement DNSBLs ce qui pourrait avoir un impact sur la livraison sur l'ensemble du service Amazon SES, ou qui pourrait avoir un impact sur la capacité à envoyer des e-mails aux destinataires qui utilisent les principaux fournisseurs de messagerie tels que Gmail, Yahoo, AOL et Hotmail. Les DNSBLs offres de 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 ceux DNSBLs qui sont peu susceptibles d'avoir un impact sur la livraison dans l'ensemble du service Amazon SES, ou ceux qui n'ont pas d'impact mesurable sur la livraison aux principaux fournisseurs de messagerie. Les offres DNSBLs de 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.

Pour les adresses IP dédiées (gérées ou standard) répertoriées dans une RBL de fournisseurs de messagerie destinataires, il n'est pas de la responsabilité de SES de la radier de la liste IPs et vous devez vous-même demander le retrait directement auprès de l'administrateur de la RBL.

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 politiques d'assistance au postmaster, vous pouvez peut-être contacter le postmaster en envoyant un e-mail à postmaster@example.com, où se [example.com](http://www.example.com) trouve le domaine en question. Les domaines sont tenus en vertu de la spécification [RFC 5321](https://tools.ietf.org/html/rfc5321) 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. Les bonnes pratiques d'envoi peuvent vous aider à garantir que vos adresses ne se retrouveront pas sur le site DNSBLs.

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 un DNSBL avec un impact significatif, comme celle de Spamhaus, les principaux fournisseurs DNSBLs de messagerie rejeteront complètement les e-mails provenant de cette adresse IP, plutôt que de les envoyer dans le dossier de spam.

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 souhaitent 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.

Statistiques d'envoi d'e-mails Amazon SES FAQs

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 traite FAQs des sujets suivants relatifs aux statistiques 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 statistiques d'ouverture et de clic pour Amazon SES à l'aide de l' CloudWatch API. Par exemple, vous pouvez utiliser le AWS CLI pour récupérer les métriques de clics à l'aide de l' CloudWatch API 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'événement”](#). Vous pouvez utiliser l'espace réservé aux pixels dans [Messagerie SMTP](#) dans 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' AWS accueil, 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'événement”](#).

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 mentionnés 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 contenus dans vos e-mails soient correctement codés URLs. Plus précisément, URLs vos liens doivent être conformes à la [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 codage incorrect se produisent généralement lorsqu' URLs ils contiennent des chaînes de requête. Par exemple, si l'URL d'un lien contenu dans votre e-mail contient un espace non codé dans la chaîne de requête (comme l'espace entre « » et John « 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 plutôt un espace codé (tel que « %20 » dans l'exemple suivant : `http://www.example). com/path/to/page? name=John%20DOE`), Amazon SES le 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](#)
 - [Configuration de open/click domaines personnalisés](#)
 - [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'événement](#)
- [Créer des filtres d'adresses IP](#)
- [Créez un pool d'adresses IP géré pour activer le service dédié IPs \(géré\)](#)
- [Créer des règles de réception](#)
- [Créez des alarmes de réputation en utilisant 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](#)

- [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 un abus de AWS ressources](#)
- [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](#)
- [Récupérez les données d'événements depuis 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 AWS SDK](#)
- [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 applications dédiées IPs](#)
- [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...
 - [Abus de AWS ressources, rapport](#)
 - [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 \(Publication d'événement\)](#)
- [FAQs \(Questions fréquemment posées\)](#)
- [Liste de suppression globale](#)

- [Champs d'en-tête, pris en charge](#)
- [Identités, gestion](#)
- [Gestion des identités et des accès](#)
- [Sécurité de l'infrastructure](#)
- [Intégrer à Amazon WorkMail Action](#)
- [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 applications dédiées IPs](#)
- [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](#)

FAQs sur les protocoles pris en charge

[Le service Amazon SES Mail Manager ajoute la prise en charge du SDK pour le protocole CBOR Smithy RPC v2 en plus du protocole JSON existant.AWS](#) Le protocole CBOR Smithy RPC v2 est plus performant que le AWS JSON pour la plupart des charges de travail. AWS SDKs priorisera le protocole le plus performant pour chaque langue.

Quels sont les protocoles CBOR AWS JSON et Smithy RPC v2, et en quoi diffèrent-ils ?

Un protocole filaire joue le rôle de médiateur entre un client et le service. Le AWS SDK gère la sérialisation (conversion d'un objet au format filaire) et la désérialisation (reconversion du format filaire en objet) entre le client et le serveur de manière transparente pour les deux protocoles.

AWS JSON - Le JSON est l'un des formats de données les plus utilisés et les plus acceptés pour la communication entre les systèmes. Ce service utilise le AWS JSON comme moyen de communication entre un client du AWS SDK et le serveur. Une requête HTTP pour une opération d'API de service accepte une entrée sous forme de JSON, l'opération est exécutée et la réponse est renvoyée au client du SDK sous forme de JSON.

Smithy RPC v2 CBOR - Le Smithy RPC v2 CBOR (Concise Binary Object Representation) est un protocole développé par Amazon pour une transmission de données plus efficace. Il s'agit d'un format de données conçu pour réduire la taille des messages et pour permettre au format d'évoluer sans nécessiter de négociation de version entre les systèmes. La principale différence par rapport au AWS JSON est que le AWS JSON utilise du texte lisible par l'homme (comme `{"name": "John"}`), tandis que le Smithy RPC v2 CBOR utilise un format binaire (séquences de 1 et de 0). Cette approche binaire crée des paquets de données plus petits qui voyagent plus rapidement sur le réseau et réduit le temps de sérialisation puisque les ordinateurs traitent directement les données binaires.

Comment démarrer avec le protocole CBOR Smithy RPC v2 ?

Pour commencer, utilisez la dernière version du AWS SDK/CLI pour utiliser le protocole CBOR Smithy RPC v2 pour ce service. Le SDK utilisera automatiquement le protocole CBOR Smithy RPC v2 lorsqu'il sera disponible. Mettez à niveau votre AWS SDK vers la version spécifiée ou vers une version ultérieure.

À compter du 16/04/2020, les modèles suivants AWS SDKs utiliseront le protocole CBOR Smithy RPC v2, tandis que les autres SDKs continueront à utiliser le protocole JSON : AWS

- AWS SDK pour C++
- AWS SDK pour Go V2
- AWS SDK pour Java 2.x
- AWS SDK pour .NET v4
- AWS Outils pour PowerShell v5
- AWS SDK pour Swift
- AWS SDK pour Kotlin

Quels sont les risques liés à l'activation du protocole CBOR Smithy RPC v2 ?

Le support supplémentaire de Smithy RPC v2 CBOR SDKs devrait être totalement transparent et facile pour les clients. Toutefois, si vous utilisez une implémentation personnalisée du AWS SDK, ou une combinaison de clients personnalisés et du SDK, qui dépend du AWS comportement de sérialisation AWS spécifique à JSON, elle peut être incompatible avec le protocole CBOR Smithy RPC v2.

Et si ma solution ne prend pas en charge Smithy RPC v2 CBOR ?

Pour utiliser le protocole AWS JSON, rétrogradez votre SDK vers une version publiée avant le 16/04/2026.

Quelles AWS régions prennent en charge le protocole CBOR Smithy RPC v2 ?

Le protocole CBOR Smithy RPC v2 est pris en charge dans toutes les [AWS régions](#) où ce service est disponible.

À quelles améliorations de latence puis-je m'attendre lors de la mise à niveau vers des versions du SDK compatibles avec Smithy RPC v2 CBOR ?

Le Smithy RPC v2 CBOR réduit la latence jusqu'à 13 % et la taille de la charge utile jusqu'à 15 % par rapport au JSON. AWS Le codage binaire élimine la surcharge liée à l'analyse de texte JSON et à l'échappement de chaînes, ce qui réduit à la fois le temps de transfert réseau et les coûts de sérialisation.

Le protocole AWS JSON sera-t-il obsolète ?

AWS Le protocole JSON continuera d'être pris en charge dans les anciennes versions de SDKs. De plus, certains langages spécifiques SDKs continueront à utiliser le AWS JSON, car il est plus performant que Smithy RPC v2 CBOR, car l'implémentation JSON disponible pour le langage est plus rapide que son implémentation CBOR.

Où puis-je trouver plus d'informations sur Smithy RPC v2 CBOR ?

Vous trouverez plus d'informations sur le protocole JSON sur le protocole AWS [AWS JSON 1.0 et le protocole AWS JSON 1.1 dans la documentation Smithy](#), et sur le [protocole Smithy RPC v2 CBOR](#) sur le protocole Smithy RPC v2 [CBOR dans la documentation Smithy](#).

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.