aws

Guía para desarrolladores

Amazon Simple Email Service

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Simple Email Service: Guía para desarrolladores

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es Amazon SES? 1
Ventajas 1
Servicios relacionados 1
Precios 2
Regiones 2
Regiones y puntos de enlace de Amazon SES 3
Aumentos del límite de envío y eliminación del entorno de pruebas 4
Verificación de direcciones de correo electrónico y dominios 4
DKIM fácil: 5
Lista de supresión a nivel de cuenta 5
Notificaciones de retroalimentación 5
Credenciales de SMTP 5
Dominios MAIL FROM personalizados 6
Autorización de envío 8
Recepción de correo electrónico 8
Cuotas 9
Cuotas de envío de correo electrónico 10
Cuotas de recepción de correo electrónico 14
Cuotas de Mail Manager 15
Cuotas generales 17
Tipos de credenciales 17
Cómo funciona Amazon SES 23
Después de que un remitente envíe una solicitud de correo electrónico a SES 24
Después de que Amazon SES envíe un correo electrónico 25
Formato de correo electrónico 27
Descripción de la capacidad de entrega 32
Prácticas recomendadas para el correo electrónico 38
Trabajando con los AWS SDK 46
Introducción 48
Configuración 48
Inscríbase en AWS 48
Configurar la cuenta de SES 49
Adjudicar acceso mediante programación (para interactuar con SES fuera de la consola) 49
Descargue un AWS SDK (para usar las API de SES) 51

Migración a Amazon SES ... 52
Paso 1. Verificar su dominio ... 52
Paso 2. Solicitar acceso de producción ... 52
Paso 3. Configurar sistemas de autenticación de dominios ... 53
Paso 4. Generar sus credenciales de SMTP ... 53
Paso 5. Conectarse a un punto de enlace de SMTP ... 53
Siguientes pasos ... 53
Solicitar acceso de producción ... 54
Límites de envío ... 59
Aumento de las cuotas de envío ... 61
Aumento automático de las cuotas de envío ... 61
El usuario solicitó un aumento de las cuotas de envío ... 62
Monitoreo de las cuotas de envío ... 63
Monitoreo de las cuotas de envío mediante la consola de Amazon SES ... 63
Monitoreo de las cuotas de envío mediante la API de Amazon SES ... 64
Errores de cuota de envío ... 65
Alcanzar límites de envío con la API de Amazon SES ... 65
Alcanzar límites de envío con SMTP ... 65
Configurar el envío de correo electrónico ... 66
Uso de la interfaz de SMTP ... 66
Requisitos para enviar correo electrónico a través de SMTP ... 67
Métodos para enviar correo electrónico a través de SMTP ... 68
Información de correo electrónico que se debe facilitar ... 68
Obtención de las credenciales de SMTP ... 69
Conexión a un punto de enlace de SMTP ... 75
Uso de paquetes de software para el envío de correo electrónico ... 76
Envío de correo electrónico mediante programación ... 78
Integración con su servidor de email existente ... 79
Prueba de la conexión a la interfaz de SMTP de Amazon SES ... 82
Uso de la API ... 85
Envío de correo electrónico con formato ... 86
Envío de correo electrónico sin procesar ... 87
Uso de plantillas para el envío de correo electrónico ... 99
Envío de correo electrónico mediante un AWS SDK ... 118
Codificaciones de contenido ... 138
Protocolos de seguridad compatibles ... 138

Remitente de correo electrónico para Amazon SES 138
Amazon SES al receptor 139
nd-to-end Cifrado electrónico 140
Campos de encabezado admitidos 141
Tipos de adjuntos no admitidos 144
Recepción de correo electrónico 146
Conceptos y casos de uso de recepción de correo electrónico 147
Control basado en destinatarios mediante reglas de recepción 147
Control basado en IP mediante filtros de dirección IP 149
Proceso de recepción de correo electrónico 150
Casos de uso y restricciones 151
Autenticación de correo electrónico y detección de malware 154
Configuración de la recepción de emails 156
Verificación de su dominio 157
Publicación de un registro MX 157
Otorgar permiso 160
Explicaciones de la consola acerca de la recepción de correo electrónico 166
Creación de reglas de recepción 166
Creación de filtros de IP 207
Métricas de recepción de correo electrónico 208
Identidades verificadas 213
Creación y verificación de identidades 213
Creación de una identidad de dominio 217
Verificación de una identidad de dominio 221
Creación de una identidad de dirección de correo electrónico 226
Verificación de una identidad de dirección de correo electrónico 228
Crear y verificar una identidad y asignar un conjunto de configuración predeterminado al mismo tiempo (API) 228
Uso de plantillas de correo electrónico de verificación personalizado 230
Administración de identidades 243
Visualización de identidades desde la consola 243
Eliminación de una identidad mediante la consola 244
Edición de una identidad mediante la consola 245
Editar una identidad para utilizar un conjunto de configuración predeterminado mediante la API 246
Recuperar el conjunto de configuración predeterminado utilizado por la identidad (API) 247

Anular el conjunto de configuración predeterminado utilizado por la identidad (API) 248
Configuración de identidades 248
Métodos de autenticación del correo electrónico 249
Configuración de notificaciones de eventos 296
Uso de la autorización de identidad 335
Uso de la autorización de envío 350
Envío de correos electrónicos de prueba con el simulador 383
Uso del simulador de buzón de correo de la consola 384
Uso del simulador de buzón de correo de forma manual 386
Conjuntos de configuración 391
Creación de conjuntos de configuración 392
Crear un conjunto de configuración 392
Cree un conjunto de configuración (AWS CLI) 396
Administrar conjuntos de configuración 398
Ver, editar y eliminar conjunto de configuración (consola) 398
Conjuntos de configuración de lista (AWS CLI) 401
Obtener los detalles del conjunto de configuración (AWS CLI) 401
Eliminar un conjunto de configuración (AWS CLI) 401
Detener el envío de correo electrónico desde un conjunto de configuración (AWS CLI) 402
Comprensión de los conjuntos de configuración predeterminados 402
Crear destinos de eventos 404
Asignar grupos de IP 409
Configuración de dominios de aperturas y clics personalizados 410
Especificación de conjuntos de configuración en el correo electrónico 417
Ver y exportar métricas de reputación 418
Habilitación de la exportación de métricas de reputación 418
Desactivación de la exportación de métricas de reputación 419
Direcciones IP dedicadas 420
Facilidad de configuración 422
Administración de la reputación 423
Capacidad de predicción de los patrones de envío 423
Volumen de correo electrónico saliente 424
Costos adicionales 424
Control sobre la reputación del remitente 425
Capacidad de aislar la reputación del remitente 425
Direcciones IP conocidas y sin cambios 425

Standard ... 426
Solicitud y renuncia ... 426
Preparación ... 431
Creación de grupos ... 434
Administradas ... 437
Beneficios y características ... 437
Importancia de la preparación ... 439
Creación de un grupo de IP administradas ... 440
Visualización del envío y la capacidad del grupo ... 444
Eliminación de un grupo de IP administradas ... 446
Traiga sus propias direcciones IP ... 447
Requisitos ... 448
Consideraciones ... 448
Uso de sus propias direcciones IP con Amazon SES ... 449
Virtual Deliverability Manager ... 450
Introducción ... 451
Introducción (consola) ... 452
Introducción (AWS CLI) ... 453
Panel de control ... 455
Uso del panel (consola) ... 458
Acceder a datos de métricas (AWS CLI) ... 463
Filtrado y exportación de datos de métricas (AWS CLI) ... 464
Búsqueda de mensajes, su estado y exportación de resultados (AWS CLI) ... 465
Administración de los trabajos de exportación (AWS CLI) ... 469
Visualización de los detalles del mensaje (AWS CLI) ... 471
Cómo se calculan las métricas del panel ... 472
Asesor ... 475
¿Qué busca el asesor ... 476
Uso del asesor (consola) ... 479
Acceso a las recomendaciones (AWS CLI) ... 480
Configuración ... 481
Cambio de la configuración de Virtual Deliverability Manager (consola) ... 481
Cambio de la configuración de Virtual Deliverability Manager (AWS CLI) ... 483
NUEVO: Mail Manager ... 485
Introducción ... 486
Introducción ... 487

Puntos finales de ingreso ... 488
Configuración de su entorno de ... 489
Crear un punto final de entrada (consola) ... 490
Políticas y declaraciones de políticas de tráfico ... 492
Creación de políticas y declaraciones de políticas de tráfico (consola) ... 493
Condiciones de la declaración de política ... 495
Conjuntos de reglas y reglas ... 495
Creación de conjuntos de reglas y reglas (consola) ... 497
Condiciones y acciones de la regla ... 498
Relé SMTP ... 501
Crear un relé SMTP (consola) ... 502
Configuración de Google Workspaces ... 506
Configuración de Microsoft Office 365 ... 508
Archivado de correo electrónico ... 514
Uso del archivado de correo electrónico (consola) ... 514
Complementos de correo electrónico ... 519
Suscribirse a Add Ons (consola) ... 520
Políticas de permisos ... 523
Políticas de puntos finales de Ingress ... 523
Políticas de retransmisión SMTP ... 525
Políticas de archivado de correo electrónico ... 526
Políticas de acción de reglas ... 532
Listas y suscripciones ... 535
Lista de supresión global ... 537
Consideraciones sobre la lista de supresión global ... 538
Uso de la lista de supresión de nivel de cuenta ... 539
Consideraciones de la lista de supresión de nivel de cuenta ... 539
Habilitar la lista de supresión de nivel de cuenta ... 541
Habilitar la lista de supresión de nivel de cuenta para un conjunto de configuración ... 542
Agregar direcciones de correo electrónico individuales a la lista de supresión de nivel de cuenta ... 544
Agregar direcciones de correo electrónico en bloque a la lista de supresión de nivel de cuenta ... 546
Ver una lista de las direcciones que están en la lista de supresión de nivel de cuenta ... 550
Eliminar de forma individual direcciones de correo electrónico de la lista de supresión de nivel de cuenta ... 553

Eliminar en bloque direcciones de correo electrónico de la lista de supresión de nivel de cuenta ... 555
Visualización de una lista de trabajos de importación de la cuenta ... 559
Obtención de información acerca de un trabajo de importación de la cuenta ... 561
Desactivar la lista de supresión de nivel de cuenta ... 562
Uso de supresión de nivel de conjunto de configuración ... 563
Habilitar la supresión de nivel de conjunto de configuración ... 566
Uso de la administración de listas ... 567
Información general acerca de la administración de listas ... 567
Configuración de la administración de listas ... 568
Tutorial de administración de listas con ejemplos ... 575
Uso de la administración de suscripciones ... 577
Información general acerca de la administración de suscripciones ... 578
Consideraciones sobre el encabezado de cancelación de suscripción ... 579
Agregar un vínculo de pie de página de cancelación de suscripción ... 580
Monitoreo de la actividad de envío ... 581
Monitoreo mediante la consola ... 588
Panel de cuenta ... 588
Métricas de reputación ... 590
Configuración de SMTP ... 591
Uso de la consola para monitorear métricas ... 592
Monitorización mediante la API ... 593
Llamada a la operación `GetSendStatistics` de la API mediante la AWS CLI ... 594
Llamada a la operación `GetSendStatistics` mediante programación ... 594
Supervisar el envío de correo electrónico mediante la publicación de eventos ... 598
Cómo funciona la publicación de eventos con los conjuntos de configuración y las etiquetas de los mensajes ... 598
Comentarios detallados para las campañas de correo electrónico ... 599
Cómo utilizar la publicación de eventos ... 601
Terminología de publicación de eventos ... 601
Configuración de la publicación de eventos ... 603
Trabajar con datos de eventos ... 619
Monitoreo de su reputación de remitente ... 694
Uso de métricas de reputación ... 694
Mensajes de métricas de reputación ... 697
Mensajes de estado general ... 697

Notificación de tasa de rebotes 699
Notificación de tasa de reclamaciones 700
Notificación de organización antispam 702
Notificación de bombardeo de lista 703
Notificaciones de retroalimentación directa 705
Notificación de lista de bloqueo de dominios 706
Notificación de revisión interna 708
Notificación de proveedor de bandeja de correo 710
Notificaciones de retroalimentación de destinatario 711
Notificación de cuenta relacionada 713
Notificación de trampa de spam 714
Notificación de sitio vulnerable 715
Notificación de credenciales comprometidas 716
Otras notificaciones 718
Creación de alarmas con CloudWatch 718
Métricas de SNDS para direcciones IP dedicadas 721
Preguntas de solución de problemas 723
Suspensión automática del envío de correo electrónico 724
En toda la cuenta 724
Para un conjunto de configuración 732
Monitorización mediante EventBridge 742
Eventos de SES 742
Referencia del esquema de eventos 744
Esquema de estado de asesor del Administrador virtual de entrega 745
Esquema de estado de envío de correo electrónico de SES 747
Usando EventBridge 749
Especifique un ejemplo de evento en EventBridge 749
Patrones de eventos para los eventos de SES 750
EventBridgeRecursos adicionales 753
Ejemplos de código 754
Amazon SES 756
Acciones 758
Escenarios 875
Ejemplos de servicios cruzados 900
Amazon SES API v2 917
Acciones 918

Escenarios 973
Seguridad 1014
Protección de datos 1015
Cifrado de datos en reposo 1016
Cifrado en tránsito 1026
Eliminación de datos personales 1026
Administración de identidades y accesos 1034
Creación de políticas de IAM para acceso a SES 1035
Ejemplos de políticas de IAM para SES 1038
AWS políticas gestionadas 1043
Uso de roles vinculados a servicios 1046
Registro y monitoreo 1049
Registro de llamadas a la API 1050
Validación de conformidad 1053
Resiliencia 1054
Seguridad de la infraestructura en SES 1055
Puntos de conexión de VPC 1055
Ejemplo del tutorial de configuración de SES en Amazon VPC 1056
Solución de problemas 1060
Problemas generales 1061
Los cambios que realizo no son visibles de inmediato 1061
Problemas de verificación 1062
Problemas de verificación del dominio 1062
Comprobación de la configuración de verificación de dominio 1064
Problemas de verificación de correo electrónico 1065
Problemas de DKIM 1066
Problemas de entrega 1068
Problemas con los correos electrónicos recibidos 1069
Problemas de notificación 1071
Errores de envío de correo electrónico 1072
Aumento del rendimiento 1075
Problemas de SMTP 1076
Códigos de respuesta de SMTP 1079
Preguntas frecuentes 1086
Preguntas frecuentes sobre el proceso de revisión de envío 1086
Cuenta en proceso de revisión 1087

Suspensión del envío 1090
Rebotes 1093
Reclamos 1097
Trampas de spam 1105
Investigaciones manuales 1107
Preguntas frecuentes acerca de la lista de agujeros negros de DNS (DNSBL) 1109
Preguntas frecuentes sobre DNSBL: P1 1110
Preguntas frecuentes sobre DNSBL: P2 1110
Preguntas frecuentes sobre DNSBL: P3 1111
Preguntas frecuentes sobre DNSBL: P4 1111
Preguntas frecuentes sobre DNSBL: P5 1111
Preguntas frecuentes sobre DNSBL: P6 1113
Preguntas frecuentes sobre métricas de correo electrónico 1114
General 1115
Seguimiento de aperturas 1116
Seguimiento de clics 1117
Índice de búsqueda rápida 1121
Instrucciones y conceptos 1121
..... mcxxviii

¿Qué es Amazon SES?

Amazon Simple Email Service (SES) es una plataforma de correo electrónico que ofrece un método sencillo y rentable de enviar y recibir correo electrónico a través de los propios dominios y direcciones de correo electrónico.

Por ejemplo, puede enviar mensajes de correo electrónico de marketing como, por ejemplo, correos electrónicos de transacciones tales como confirmaciones de pedidos y otros tipos de correspondencia tales como boletines. Al utilizar Amazon SES para recibir correo, puede desarrollar soluciones de software como, por ejemplo, agentes de respuesta automática de correo electrónico, sistemas de anulación de suscripción a correo electrónico y aplicaciones que generan tickets del servicio de atención al cliente a partir de correos electrónicos entrantes.

Para obtener más información acerca de los temas relacionados con Amazon SES, consulte el Blog de mensajería y segmentación de AWS.

Ventajas

Construir una solución de correo electrónico a gran escala supone a menudo un reto complejo y caro para una empresa. Debe enfrentarse a muchos problemas de infraestructura, como la administración del servidor de email, la configuración de la red o la reputación de la dirección IP. Además, las soluciones de correo electrónico de terceros requieren negociaciones de contractos y precios, así como costos significativos por adelantado. Amazon SES elimina estos desafíos y le permite beneficiarse de los años de experiencia y la sofisticada infraestructura de correo electrónico que Amazon.com ha construido para atender a su propia base de clientes a gran escala.

Servicios relacionados

Amazon SES se integra perfectamente con otros AWS productos. Por ejemplo, puede hacer lo siguiente:

- Añadir capacidades de envío de correo electrónico a cualquier aplicación.
- Puede enviar correos electrónicos desde Amazon EC2 mediante un SDK de AWS, mediante la interfaz de SMTP de Amazon SES o realizando llamadas directamente a la API de Amazon SES.
- Utilizar AWS Elastic Beanstalk para crear aplicaciones habilitadas para correo electrónico, tales como un programa que utilice Amazon SES para enviar un boletín a los clientes.

- Configurar Amazon Simple Notification Service (Amazon SNS) para recibir notificaciones de los correos electrónicos rebotados, que han generado un reclamo o que se han entregado correctamente al servidor de correo del destinatario. Cuando se usa Amazon SES para recibir correos electrónicos, el contenido del correo electrónico se puede publicar en temas de Amazon SNS.
- Úselo AWS Management Console para configurar Easy DKIM, que es una forma de autenticar sus correos electrónicos. Aunque puede utilizar Easy DKIM con cualquier proveedor de DNS, su configuración resulta especialmente sencilla si administra el dominio con Route 53.
- Controlar el acceso de los usuarios a su envío de correo electrónico mediante AWS Identity and Access Management (IAM).
- Almacenar los mensajes de correo electrónico que reciba en Amazon Simple Storage Service (Amazon S3).
- Realizar acciones en los correos electrónicos recibidos desencadenando funciones de AWS Lambda.
- Utilizar AWS Key Management Service (AWS KMS) para cifrar opcionalmente el correo que reciba en el bucket de Amazon S3.
- Utilizar AWS CloudTrail para registrar llamadas a la API de Amazon SES que realiza mediante la consola o la API de Amazon SES.
- Publica tu correo electrónico enviando eventos a Amazon CloudWatch o Amazon Data Firehose. Si publicas tus eventos de envío de correo electrónico en Firehose, puedes acceder a ellos en Amazon Redshift, OpenSearch Amazon Service o Amazon S3.

Precios

Con Amazon SES, el pago se basa en el volumen de mensajes de correo electrónico enviados y recibidos. Para obtener más información, consulte Precios de Amazon SES.

Regiones y Amazon SES

Amazon SES está disponible en varias AWS regiones del mundo. Dentro de cada región, AWS mantiene varias zonas de disponibilidad. Estas zonas de disponibilidad están físicamente aisladas entre sí, pero están unidas mediante conexiones de red privadas con un alto nivel de rendimiento y redundancia y con baja latencia. Estas zonas de disponibilidad nos permiten ofrecer unos niveles muy altos de disponibilidad y redundancia y minimizar la latencia.

Para obtener una lista de todos los puntos de conexión regionales de Amazon SES, consulte Puntos de conexión y cuotas de Amazon Simple Email Service en la Referencia general de AWS. Para obtener más información sobre la cantidad de zonas de disponibilidad de cada región, consulte Infraestructura global de AWS.

Esta sección contiene la información que necesita saber si planea usar Amazon SES en varias AWS regiones. En él se explican los siguientes temas:

- Regiones y puntos de enlace de Amazon SES
- Aumentos del límite de envío y eliminación del entorno de pruebas
- Verificación de direcciones de correo electrónico y dominios
- DKIM fácil:
- Lista de supresión a nivel de cuenta
- Notificaciones de retroalimentación
- Credenciales de SMTP
- Autorización de envío
- Dominios MAIL FROM personalizados
- Recepción de correo electrónico
- Configuración de registros (MX)

Para obtener información general sobre AWS las regiones, consulte los puntos AWS de enlace del servicio en la Referencia AWS general.

Regiones y puntos de enlace de Amazon SES

Al utilizar Amazon SES para enviar correo electrónico, se conecta a una URL que proporciona un punto de conexión para la API de SES o la interfaz de SMTP. La Referencia general de AWS contiene una lista completa de los puntos de conexión que se utilizan para enviar y recibir correo electrónico a través de Amazon SES. Para obtener más información, consulte Puntos de conexión y cuotas de Amazon Simple Email Service en la Referencia general de AWS.

Cuando se envía correo electrónico a través de Amazon SES, se pueden utilizar las direcciones URL en las filas especificadas con HTTPS en la columna Protocol para realizar solicitudes de HTTPS a la API de SES. También puede usar las direcciones URL en las filas especificadas con SMTP en la columna Protocol para enviar correo electrónico mediante la interfaz de SMTP.

Si ha configurado Amazon SES para recibir el correo electrónico que se envía a su dominio, puede usar las direcciones URL de los puntos de enlace SMTP de entrada (es decir, las URL que comienzan con “inbound-smtp.”) al configurar los registros de intercambio de correo (MX) en la configuración de DNS de su dominio.

> **Note**
>
> Las direcciones URL de SMTP de entrada no son direcciones de servidores IMAP. Es decir, no las puede usar para recibir correo electrónico mediante una aplicación, como Outlook. Para ver un servicio que proporciona un servidor IMAP para el correo entrante, consulta Amazon WorkMail.

Aumentos del límite de envío y eliminación del entorno de pruebas

El estado de entorno limitado de su cuenta puede variar AWS de una región a otra. Es decir, aunque su cuenta se haya eliminado del entorno de pruebas en la región EE. UU. Oeste (Oregón), puede seguir presente en el entorno de pruebas de la región EE. UU. Este (Norte de Virginia), a no ser que también lo haya eliminado del entorno de pruebas de esta última.

Los límites de envío también pueden variar según la AWS región. Por ejemplo, si su cuenta puede enviar 10 mensajes por segundo en la región Europa (Irlanda), en otras regiones es posible que pueda enviar más o menos mensajes.

Cuando envíe una solicitud para que su cuenta se elimine del entorno de pruebas o envíe una solicitud para aumentar las cuotas de envío de su cuenta, asegúrese de elegir todas las regiones de AWS a las que se aplique dicha solicitud. Puede enviar varias solicitudes en un mismo caso del Centro de soporte.

Verificación de direcciones de correo electrónico y dominios

Para poder enviar correo electrónico mediante Amazon SES, debe verificar que es el propietario de la dirección de correo electrónico o del dominio desde los que desea realizar el envío. El estado de verificación de las direcciones de correo electrónico y los dominios también varía según la AWS región. Por ejemplo, si verifica un dominio en la región EE. UU. Oeste (Oregón), no podrá usar ese dominio para enviar correo electrónico en la región EE. UU. Este (Norte de Virginia) hasta que haya completado de nuevo el proceso de verificación para esa región. Para obtener información acerca de la verificación de direcciones de correo electrónico y dominios, consulte Identidades verificadas en Amazon SES.

DKIM fácil:

Debe realizar el proceso de configuración de Easy DKIM para cada región en la que desea utilizar Easy DKIM. Es decir, en cada región, tiene que usar la consola de Amazon SES o la API de Amazon SES para generar registros TXT. A continuación, debe añadir todos los registros TXT a la configuración de DNS del dominio. Para obtener más información acerca de la configuración de Easy DKIM, consulte Easy DKIM en Amazon SES.

Lista de supresión a nivel de cuenta

Tu lista de supresión a nivel de cuenta de Amazon SES Cuenta de AWS solo se aplica a la actual. Región de AWS Puede agregar o eliminar direcciones de forma manual, ya sea de manera individual o masiva, en la lista de supresión a nivel de cuenta mediante la API v2 de SES o la consola. Para obtener más información acerca del uso de la lista de supresión a nivel de cuenta, consulte Uso de la lista de supresión de nivel de cuenta de Amazon SES.

Notificaciones de retroalimentación

Existen dos puntos importantes que deben tenerse en cuenta acerca de cómo configurar las notificaciones de retroalimentación en varias regiones:

- La configuración de identidad verificada, como, por ejemplo, si recibe retroalimentación por correo electrónico o por medio de Amazon Simple Notification Service (Amazon SNS), solo se aplica a la región en la que se define. Por ejemplo, si verifica user@example.com en las regiones EE. UU. Oeste (Oregón) y EE. UU. Este (Norte de Virginia), y desea recibir correos electrónicos rebotados por medio de notificaciones de Amazon SNS, debe utilizar la API de Amazon SES o la consola de Amazon SES para configurar las notificaciones de retroalimentación de Amazon SNS para user@example.com en ambas regiones.
- Los temas de Amazon SNS que utilice para el reenvío de retroalimentación deben encontrarse en la misma región en la que se utilice Amazon SES.

Credenciales de SMTP

Las credenciales que utiliza para enviar correos electrónicos a través de la interfaz SMTP de Amazon SES son exclusivas de cada AWS región. Si utiliza la interfaz de SMTP de Amazon SES para enviar correo electrónico en más de una región, tiene que generar un conjunto de credenciales de SMTP para cada región.

> **Note**
>
> Si creó sus credenciales SMTP antes del 10 de enero de 2019, sus credenciales SMTP se crearon con una versión anterior de Signature. AWS Por motivos de seguridad, debe eliminar las credenciales que creó antes de esa fecha y reemplazarlas por otras nuevas. Puede eliminar las credenciales antiguas mediante la consola de IAM.

Dominios MAIL FROM personalizados

Puede utilizar el mismo dominio MAIL FROM personalizado para identidades verificadas en distintas regiones de AWS . Si es lo que desea hacer, solo tiene que publicar un único registro MX en el servidor DNS para el dominio MAIL FROM. En esta situación, las notificaciones de rebotes se envían al punto de enlace de retroalimentación de Amazon SES de la región que ha especificado en primer lugar en el registro MX. A continuación, Amazon SES redirige los rebotes a la identidad verificada de la región que envió el mensaje de correo electrónico.

Utilice la configuración del registro MX que proporciona Amazon SES durante el proceso de configuración MAIL FROM personalizada para una identidad en una de las regiones. El proceso de configuración MAIL FROM personalizado se describe en Uso de un dominio MAIL FROM personalizado. Como referencia, puede buscar los puntos de enlace de retroalimentación de todas las regiones en la siguiente tabla.

Nombre de la región	Puntos de enlace de retroalimentación para configuraciones de envío MAIL FROM personalizadas
Este de EE. UU. (Ohio)	feedback-smtp.us-east-2.amazonses.com
Este de EE. UU. (Norte de Virginia)	feedback-smtp.us-east-1.amazonses.com
Oeste de EE. UU. (Norte de California)	feedback-smtp.us-west-1.amazonses.com
Oeste de EE. UU. (Oregón)	feedback-smtp.us-west-2.amazonses.com
África (Ciudad del Cabo)	feedback-smtp.af-south-1.amazonses.com
Asia-Pacífico (Yakarta)	feedback-smtp.ap-southeast-3.amazonses.com

Nombre de la región	Puntos de enlace de retroalimentación para configuraciones de envío MAIL FROM personalizadas
Asia-Pacífico (Bombay)	feedback-smtp.ap-south-1.amazonses.com
Asia-Pacífico (Osaka)	feedback-smtp.ap-northeast-3.amazonses.com
Asia-Pacífico (Seúl)	feedback-smtp.ap-northeast-2.amazonses.com
Asia-Pacífico (Singapur)	feedback-smtp.ap-southeast-1.amazonses.com
Asia-Pacífico (Sídney)	feedback-smtp.ap-southeast-2.amazonses.com
Asia-Pacífico (Tokio)	feedback-smtp.ap-northeast-1.amazonses.com
Canadá (centro)	feedback-smtp.ca-central-1.amazonses.com
Europa (Fráncfort)	feedback-smtp.eu-central-1.amazonses.com
Europa (Irlanda)	feedback-smtp.eu-west-1.amazonses.com
Europa (Londres)	feedback-smtp.eu-west-2.amazonses.com
Europa (Milán)	feedback-smtp.eu-south-1.amazonses.com
Europa (París)	feedback-smtp.eu-west-3.amazonses.com
Europa (Estocolmo)	feedback-smtp.eu-north-1.amazonses.com
Israel (Tel Aviv)	feedback-smtp.il-central-1.amazonses.com
Medio Oriente (Baréin)	feedback-smtp.me-south-1.amazonses.com
América del Sur (São Paulo)	feedback-smtp.sa-east-1.amazonses.com
AWS GovCloud (EE. UU. al oeste)	feedback-smtp. us-gov-west-1.amazonses.com
AWS GovCloud (Este de EE. UU.)	feedback-smtp. us-gov-east-1.amazonses.com

Autorización de envío

Los remitentes delegados solo pueden enviar correos electrónicos desde la AWS región en la que se haya verificado la identidad del propietario de la identidad. La política de autorización de envío que otorga permiso al remitente delegado debe estar asociada a la identidad en dicha región. Para obtener más información acerca de la autorización de envío, consulte Uso de la autorización de envío con Amazon SES.

Recepción de correo electrónico

Con la excepción de los buckets de Amazon S3, todos los AWS recursos que utilice para recibir correos electrónicos con Amazon SES deben estar en la misma AWS región que el punto de conexión de Amazon SES. Por ejemplo, si utiliza Amazon SES en la región EE. UU. Oeste (Oregón), cualquier tema de Amazon SNS, clave de AWS KMS y función de Lambda que utilice también deben estar en la región EE. UU. Oeste (Oregón). Del mismo modo, para recibir correo electrónico con Amazon SES dentro de una región, debe crear un conjunto de reglas de recepción activas en esa región.

En la siguiente tabla se enumeran los puntos de enlace de recepción de correo electrónico de todas AWS las regiones en las que Amazon SES admite la recepción de correo electrónico:

Nombre de la región	Región	Punto de conexión de recepción de correo electrónico
Este de EE. UU. (Norte de Virginia)	us-east-1	inbound-smtp.us-east-1.amazonaws.com
Este de EE. UU. (Ohio)	us-east-2	inbound-smtp.us-east-2.amazonaws.com
Oeste de EE. UU. (Oregón)	us-west-2	inbound-smtp.us-west-2.amazonaws.com
Asia-Pacífico (Yakarta)	ap-southeast-3	inbound-smtp.ap-southeast-3.amazonaws.com
Asia Pacífico (Singapur)	ap-southeast-1	inbound-smtp.ap-southeast-1.amazonaws.com

Nombre de la región	Región	Punto de conexión de recepción de correo electrónico
Asia Pacífico (Sídney)	ap-southeast-2	inbound-smtp.ap-southeast-2.amazonaws.com
Asia Pacífico (Tokio)	ap-northeast-1	inbound-smtp.ap-northeast-1.amazonaws.com
Canadá (Central)	ca-central-1	inbound-smtp.ca-central-1.amazonaws.com
Europa (Frankfurt)	eu-central-1	inbound-smtp.eu-central-1.amazonaws.com
Europa (Irlanda)	eu-west-1	inbound-smtp.eu-west-1.amazonaws.com
Europa (Londres)	eu-west-2	inbound-smtp.eu-west-2.amazonaws.com

SES no admite la recepción de correos electrónicos en las siguientes regiones: EE. UU. Oeste (Norte de California), África (Ciudad del Cabo), Asia Pacífico (Mumbai), Asia Pacífico (Osaka), Asia Pacífico (Seúl), Europa (Milán), Europa (París), Europa (Estocolmo), Israel (Tel Aviv), Oriente Medio (Bahréin), Sudamérica (São Paulo), AWS GovCloud (EE. UU. oeste) y AWS GovCloud (EE. UU. Este).

Cuotas de servicio de Amazon SES

En las siguientes secciones, se enumeran y describen las cuotas que se aplican a los recursos y las operaciones de Amazon SES. Algunas cuotas pueden aumentarse, mientras que otras no. Para determinar si puede solicitar un aumento de una cuota, consulte la columna Adjustable (Ajustable).

> **Note**
>
> Las cuotas de SES son para cada uno de Región de AWS los que utilices en tu. Cuenta de AWS

Cuotas de envío de correo electrónico

Se aplican las siguientes cuotas al envío de correo electrónico a través de SES.

Cuotas de envío

Las cuotas se basan en el número de destinatarios y no en el número de mensajes.

Recurso	Cuota predeterminada	Ajustable
Número de correos electrónicos que pueden enviarse cada 24 horas	Si su cuenta está en el entorno de pruebas, puede enviar hasta 200 mensajes de correo electrónico cada 24 horas. Si su cuenta está fuera del entorno de pruebas, este número varía en función de su caso de uso específico.	Sí
Número de correos electrónicos que pueden enviarse por segundo (tasa de envío)	Si su cuenta está en el entorno de pruebas, puede enviar 1 correo electrónico por segundo. Si su cuenta está fuera del entorno de pruebas, esta tasa varía en función de su caso de uso específico.	Sí

Cuotas de mensajes

Recurso	Cuota predeterminada	Ajustable
Uso de API v1 de SES: el tamaño máximo de mensaje (incluidos los archivos adjuntos)	10 MB por mensaje (en codificación Base64).	No (Para cargas de trabajo con tamaños de mensaje superiores a 10 MB, considere la posibilidad de migrar a la API v2 de SES).
Uso de la API v2 de SES o SMTP: el tamaño máximo de mensaje (incluidos los archivos adjuntos)	40 MB por mensaje (en codificación Base64).	No

> **Note**
>
> Los mensajes de más de 10 MB están sujetos a la limitación del ancho de banda y, según la velocidad de envío, es posible que se limite a 40 MB/s. Por ejemplo, podría enviar un mensaje de 40 MB a una velocidad de 1 mensaje por segundo o dos mensajes de 20 MB por segundo.

Cuotas de los remitentes y destinatarios

Recurso	Cuota predeterminada	Ajustable
Número máximo de destinatarios por mensaje	50 destinatarios por mensaje. **Note** Un destinatario es cualquier dirección "To", "CC" o "BCC".	Este límite de destinatario no se puede ajustar. Póngase en contacto con su administrador de AWS cuentas para solicitar esta función después de leer la siguiente nota.

Recurso	Cuota predeterminada	Ajustable
Número máximo de identidad es que puede verificar	10 000 identidades por Región de AWS. **Note** Una identidad es un dominio o dirección de correo electrónico que se utiliza para enviar correos electrónicos a través de SES.	Póngase en contacto con el administrador de la cuenta de AWS para analizar su caso de uso.
Cantidad máxima de grupos de IP dedicados (incluidos los grupos de IP administrados y estándar)	50	No

Note

Antes de solicitar un aumento del límite de destinatarios por mensaje, lea este blog y prepárese para describir detalladamente por qué su caso de uso no puede utilizarse con el límite predeterminado de 50 destinatarios por mensaje o mediante el envío de mensajes a destinatarios individuales. Definir varios destinatarios en el destino de un mensaje puede dar lugar a una observabilidad y una capacidad de entrega deficientes, por lo que no debe utilizarse a menos que su caso de uso lo requiera específicamente.

Cuotas relacionadas con la publicación de eventos

Recurso	Cuota predeterminada	Ajustable
Número máximo de conjuntos de configuración	10 000	No

Recurso	Cuota predeterminada	Ajustable
Longitud máxima del nombre del conjunto de configuración	Los nombres del conjunto de configuración pueden contener hasta 64 caracteres alfanuméricos. También pueden contener guiones (-) y guiones bajos (_). Los nombres no pueden contener espacios, caracteres acentuados ni ningún otro carácter especial.	No
Número máximo de destinos de evento por conjunto de configuración	10	No
Número máximo de dimensiones por destino CloudWatch del evento	10	No

Cuotas de plantillas de correo electrónico

Recurso	Cuota predeterminada	Ajustable
Número máximo de plantillas de correo electrónico en cada una Región de AWS	20 000	No
Tamaño máximo de la plantilla	500 KB	No
Número máximo de valores de sustitución en cada plantilla	Sin límite	N/A
Número máximo de destinatarios para cada correo electrónico con plantilla	50 destinos. Un destino es cualquier dirección de correo	No

Recurso	Cuota predeterminada	Ajustable
	electrónico en los campos "Para", "CC" o "CCO". **Note** El número de destinos con los que puede ponerse en contacto en una única llamada a la API podría estar limitado por la tasa de envío máxima de su cuenta.	

Cuotas de recepción de correo electrónico

La siguiente tabla muestra las cuotas asociadas a la recepción de correo electrónico a través de SES.

Recurso	Cuota predeterminada	Ajustable
Número máximo de reglas por conjunto de reglas de recepción	200	No
Número máximo de acciones por regla de recepción	10	No
Número máximo de destinatarios por regla de recepción	100	No
Número máximo de conjuntos de reglas de recepción por Cuenta de AWS	40	No

Recurso	Cuota predeterminada	Ajustable
Número máximo de filtros de direcciones IP por Cuenta de AWS	100	No
Tamaño máximo de email (incluidos encabezados) que se puede almacenar en un bucket de Amazon S3	40 MB	No
Tamaño máximo de email (incluidos encabezados) que se puede publicar mediante una notificación de Amazon SNS	150 KB	No

Cuotas de Mail Manager

En la siguiente tabla se muestran las cuotas asociadas a Mail Manager.

Recurso	Cuota predeterminada	Ajustable
Número máximo de puntos finales de entrada abiertos	10	No
Número máximo de puntos finales de entrada autorizados	50	No
Número máximo de destinatarios por mensaje	100	No
Tamaño máximo del correo electrónico (incluidos los encabezados)	40 MB	No
Número máximo de declaraciones de política de tráfico	20	No

Recurso	Cuota predeterminada	Ajustable
Número máximo de condiciones de la declaración de política de tráfico	10	No
Número máximo de políticas de tráfico por región	100	No
Número máximo de relés SMTP	100	No
Número máximo de conjuntos de reglas	40	No
Número máximo de ejecuciones de reglas por mensaje	200	No
Número máximo de condiciones por regla	10	No
Número máximo de acciones por regla	10	No
Número máximo de acciones de retransmisión o envío por conjunto de reglas	10	No
Número máximo de archivos activos	10	No
Número máximo de solicitudes de búsqueda en ejecución en paralelo	1	No
Número máximo de solicitudes de exportación en ejecución en paralelo	1	No

Recurso	Cuota predeterminada	Ajustable
Número máximo de cambios de retención para el archivo por semana	1	No

Cuotas generales

La siguiente tabla muestra las cuotas que se aplican tanto al envío como a la recepción de correo electrónico a través de SES.

Cuotas de envío de la API de SES

Recurso	Cuota predeterminada	Ajustable
Velocidad a la que puede llamar a acciones de la API de Amazon SES	Todas las acciones (excepto `SendEmail` , `SendRawEmail` y `SendTemplatedEmail`) están limitadas a una solicitud por segundo.	No
Partes MIME	500	No

Tipos de credenciales de Amazon SES

Para interactuar con Amazon Simple Email Service (Amazon SES), debe utilizar credenciales de seguridad a fin de verificar su identidad y si tiene permiso para interactuar con Amazon SES. Existen distintos tipos de credenciales y las credenciales que utilice dependerán de lo que desea hacer. Por ejemplo, utilice las claves de acceso de AWS al enviar un correo electrónico mediante la API de Amazon SES y las credenciales de SMTP cuando envíe un correo electrónico mediante la interfaz de SMTP de Amazon SES.

La siguiente tabla muestra los tipos de credenciales que puede utilizar con Amazon SES, en función de lo que esté haciendo.

Si desea acceder a...	Utilice estas credenciales	De qué constan las credenciales	Cómo obtener las credencia les
API de Amazon SES (Puede tener acceso a la API de Amazon SES directa o indirecta mente a través de un SDK de AWS, AWS Command Line Interface o AWS Tools for Windows PowerShell).	Claves de acceso de AWS	ID de clave de acceso y clave de acceso secreta	Consulte Access Keys en la Referencia general de AWS. **Note** Como práctica recomendada de seguridad, utilice las claves de acceso de usuario de AWS Identity and Access Management (IAM) en lugar de las claves de acceso de Cuenta de AWS. Las credencia les de su Cuenta de AWS le conceden acceso completo a todos los recursos de AWS, por lo que debería almacenarlos en un lugar seguro y utilizar las credencia les de usuario de IAM para interactu ar a diario con AWS. Para obtener más información, consulte Credenciales de cuenta raíz frente a credenciales de usuario de IAM en la

Si desea acceder a...	Utilice estas credenciales	De qué constan las credenciales	Cómo obtener las credencia les
			Referencia general de AWS.

Si desea acceder a...	Utilice estas credenciales	De qué constan las credenciales	Cómo obtener las credencia les
Interfaz de SMTP de Amazon SES	Credenciales de SMTP	Nombre de usuario y contraseña	Consulte Obtención de las credenciales de SMTP de Amazon SES. **Note** Aunque las credencia les de SMTP de Amazon SES son diferentes de las claves de acceso de AWS y las claves de acceso de usuario de IAM, las credenciales de SMTP de Amazon SES son en realidad un tipo de credencia les de IAM. Un usuario de IAM puede crear credenciales de SMTP de Amazon SES, pero el propietario de la cuenta raíz debe garantizar que la política de usuario de IAM les otorgue permiso para acceder a las siguientes acciones de IAM: “iam:ListUsers”, “iam:CreateUser”, “iam:CreateAccessK

Si desea acceder a...	Utilice estas credenciales	De qué constan las credenciales	Cómo obtener las credencia les
			ey” e “iam:PutU serPolicy”.

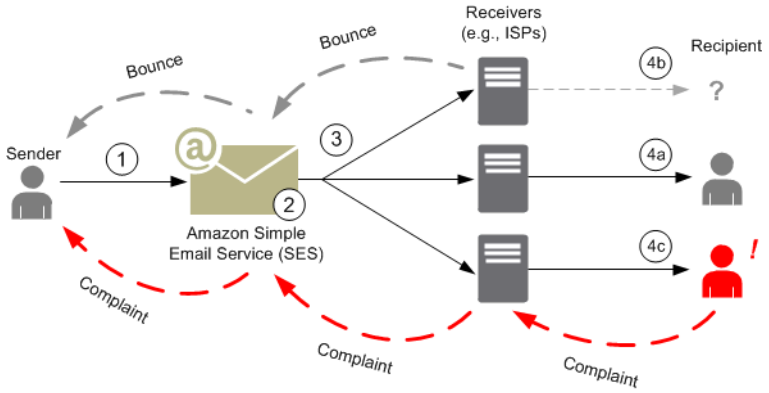
Si desea acceder a...	Utilice estas credenciales	De qué constan las credenciales	Cómo obtener las credencia les
Consola de Amazon SES	Nombre de usuario y contraseña de IAM O BIEN Dirección de correo electrónico y contraseña	Nombre de usuario y contraseña de IAM O BIEN Dirección de correo electrónico y contraseña	Consulte Nombre de usuario y contraseña de IAM y Correo electrónico y contraseña en la Referencia general de AWS. **Note** Como práctica recomendada de seguridad, utilice un nombre de usuario y una contraseñ a de IAM en lugar de una dirección de correo electróni co y una contraseñ a. La combinaci ón de dirección de correo electrónico y contraseña son para su Cuenta de AWS, por lo que ha de almacenarlos en un lugar seguro en lugar de utilizarlos para la interacción diaria con AWS. Para obtener más información, consulte Credencia les de cuenta raíz frente a credenciales de usuario de IAM en

Si desea acceder a...	Utilice estas credenciales	De qué constan las credenciales	Cómo obtener las credencia les
			la Referencia general de AWS.

Para obtener más información acerca de los distintos tipos de credenciales de seguridad de AWS (excepto las credenciales de SMTP, que se utilizan solo para Amazon SES), consulte Credenciales de seguridad de AWS en la Referencia general de AWS.

Cómo funciona el envío de correo electrónico en Amazon SES

Este tema describe lo que ocurre cuando se envía un correo electrónico con SES y los diferentes resultados que se pueden producir después de que se envíe el correo electrónico. La siguiente figura es información general de alto nivel acerca del proceso de envío:



1. Una aplicación cliente, que actúa como un remitente de correo electrónico, realiza una solicitud a SES para enviar correo electrónico a uno o varios destinatarios.
2. Si la solicitud es válida, SES acepta el correo electrónico.
3. SES envía el mensaje a través de Internet al receptor del destinatario. Una vez que el mensaje se transfiere a SES, se suele enviar inmediatamente, con el primer intento de entrega normalmente en un plazo de milisegundos.
4. En este momento, existen diferentes posibilidades. Por ejemplo:
    a. El ISP entrega correctamente el mensaje en la bandeja de entrada del destinatario.

b. La dirección de correo electrónico del destinatario no existe, por lo que el ISP envía una notificación de rebote a SES. SES, a continuación, reenvía la notificación al remitente.

c. El destinatario recibe el mensaje, pero lo considera spam y registra una reclamación en el ISP. El ISP, que tiene un bucle de retroalimentación configurado con SES, envía la reclamación a SES, que a su vez la reenvía al remitente.

En las secciones siguientes se revisan los posibles resultados individuales después de que un remitente envíe una solicitud de correo electrónico a SES y después de que SES envíe un mensaje de correo electrónico al destinatario.

Después de que un remitente envíe una solicitud de correo electrónico a SES

Cuando el remitente realiza una solicitud a SES para enviar un correo electrónico, la llamada puede tener éxito o producir un error. En las secciones siguientes se describe lo que ocurre en cada caso.

Solicitud de envío correcta

Si la solicitud a SES se realiza correctamente, SES devuelve una respuesta de operación correcta al remitente. Este mensaje incluye el ID de mensaje, una cadena de caracteres que identifica de forma única la solicitud. Puede usar el ID del mensaje para identificar el correo electrónico enviado o realizar un seguimiento de los problemas encontrados durante el envío (debe almacenar su propio mapeo entre un identificador y el ID del mensaje de SES que SES le transfiere de vuelta cuando acepta el correo electrónico). A continuación, SES crea un mensaje de correo electrónico basado en los parámetros de solicitud, analiza el mensaje para detectar contenido dudoso y virus y, a continuación, lo envía a través de Internet con Simple Mail Transfer Protocol (SMTP). Su mensaje suele enviarse inmediatamente; el primer intento de entrega suele hacerse efectivo en milisegundos.

> **Note**
>
> Si SES acepta la solicitud del remitente y, a continuación, determina que el mensaje contiene un virus, SES deja de procesar el mensaje y no intenta enviarlo al servidor de correo del destinatario.

Solicitud de envío con error

Si la solicitud de envío de correo electrónico del remitente a SES produce un error, SES responde al remitente con un error y anula el correo electrónico. La solicitud podría generar un error por varios motivos. Por ejemplo, la solicitud podría no tener el formato correcto o es posible que el remitente no haya verificado la dirección de correo electrónico.

El método a través del que puede determinar si la solicitud ha producido un error depende de cómo llame a SES. Los siguientes son ejemplos de cómo se devuelven los errores y excepciones:

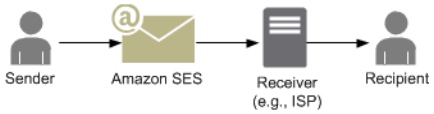
- Si llama a SES a través de la API de consultas (HTTPS) (`SendEmail` o `SendRawEmail`), las acciones devolverán un error. Para obtener más información, consulte la Referencia de la API de Amazon Simple Email Service.
- Si utiliza un SDK de AWS para un lenguaje de programación que emplea excepciones, la llamada a SES lanzará una excepción MessageRejectedException. (El nombre de la excepción puede variar ligeramente en función del SDK).
- Si utiliza la interfaz de SMTP, el remitente recibe un código de respuesta de SMTP, pero la forma en que se transmite el error depende del cliente del remitente. Algunos clientes podrían mostrar un código de error, mientras que otros no.

Para obtener información acerca de los errores que se pueden producir al enviar un correo electrónico con SES, consulte Errores de envío de correo electrónico de Amazon SES.

Después de que Amazon SES envíe un correo electrónico

Si la solicitud del remitente a SES se realiza correctamente, SES envía el correo electrónico y se da uno de los siguientes resultados:

- Entrega correcta y el destinatario no se opone al correo electrónico: el ISP acepta el correo electrónico y lo entrega al destinatario. En la siguiente ilustración se muestra una entrega correcta.



- Devolución permanente: el ISP rechaza este correo electrónico debido a una condición persistente o SES lo rechaza porque la dirección de correo electrónico está en la lista de supresión de SES. Una dirección de correo electrónico está en la lista de supresión de SES si ha provocado recientemente una devolución permanente para cualquier cliente de SES. Un rebote permanente

con un ISP puede ocurrir porque la dirección del destinatario no sea válida. Una notificación de devolución permanente se envía desde el ISP de nuevo a SES, que informa al remitente a través de correo electrónico o a través de Amazon Simple Notification Service (Amazon SNS), en función de la configuración del remitente. SES notifica al remitente los rebotes de la lista de supresión por el mismo medio. La ruta de un rechazo permanente de un ISP se muestra en la siguiente ilustración.

- Devolución temporal: el ISP no puede entregar el correo electrónico al destinatario por un problema temporal, por ejemplo, si el ISP está demasiado ocupado para gestionar la solicitud o si el buzón del destinatario está lleno. Un rebote temporal también puede ocurrir si el dominio no existe. El ISP envía una notificación de devolución temporal de vuelta a SES o, en el caso de un dominio inexistente, SES no puede encontrar un servidor de correo electrónico para el dominio. En cualquier caso, SES vuelve a intentar el correo electrónico durante un periodo de tiempo prolongado. Si SES no puede entregar el correo electrónico en ese periodo, le envía una notificación de rebote por correo electrónico o a través de Amazon SNS. Si SES puede entregar el correo electrónico al destinatario durante un reintento, la entrega se realiza correctamente. En la siguiente ilustración se muestra un rebote temporal. En este caso, SES vuelve a intentar enviar el correo electrónico y el ISP puede finalmente entregarlo al destinatario.

- Reclamación: el ISP acepta el correo electrónico y se entrega al destinatario, pero el destinatario considera que el correo electrónico es spam y hace clic en un botón como "Mark as spam" (Marcar como spam) en su cliente de correo electrónico. Si SES tiene un bucle de retroalimentación configurado con el ISP, entonces se envía una notificación de reclamación a SES, que a su vez reenvía la notificación de reclamación al remitente. La mayoría de los ISP no proporcionan la dirección de correo electrónico del destinatario que presentó la reclamación, por lo que la reclamación de SES ofrece al remitente una lista de destinatarios que podrían haber enviado la reclamación, en función de los destinatarios del mensaje original y el ISP desde el que SES recibió la reclamación. La ruta de una reclamación se muestra en la siguiente ilustración.

- Respuesta automática: el ISP acepta el correo electrónico y lo envía al destinatario. El ISP envía a continuación una respuesta automática, por ejemplo un mensaje de fuera de la oficina (OOTO) a SES. SES reenvía la notificación de respuesta automática al remitente. En la figura siguiente se muestra una respuesta automática.

  Asegúrese de que el programa habilitado para SES no reintente el envío de mensajes que generen una respuesta automática.

> **Tip**
>
> Puede utilizar el simulador de bandeja de correo de SES para probar una entrega correcta, rebote, reclamación, OOTO o lo que ocurre cuando una dirección está en la lista de supresión. Para obtener más información, consulte Uso del simulador de buzón de correo de forma manual.

Formato de correo electrónico y Amazon SES

Cuando un cliente realiza una solicitud a Amazon SES, Amazon SES crea un mensaje de correo electrónico que cumple la especificación de formato de mensajes de Internet (RFC 5322). Un correo electrónico se compone de un encabezado, un cuerpo y un sobre, tal y como se describe a continuación.

- Encabezado: contiene instrucciones de enrutamiento e información acerca del mensaje. Algunos ejemplos son la dirección del remitente, la dirección del destinatario, el asunto y la fecha. El encabezado es análogo a la información de la parte superior de una carta postal, aunque puede contener muchos otros tipos de información, como el formato del mensaje.
- Cuerpo: contiene el texto del propio mensaje.
- Sobre: contiene la información de enrutamiento real que se comunica entre el cliente de correo electrónico y el servidor de correo durante la sesión SMTP. Esta información de sobre de correo electrónico es análoga a la información en un sobre postal. La información de enrutamiento del sobre de correo electrónico suele ser la misma que la información de enrutamiento en el encabezado de correo electrónico, pero no siempre. Por ejemplo, cuando se envía una copia oculta (CCO), la dirección de destinatario real (tomada del sobre) no es la misma que la dirección

de destinatario ("Para") que se muestra en el cliente de correo electrónico del destinatario, que se toma del encabezado.

A continuación se muestra un ejemplo sencillo de un correo electrónico. El encabezado va seguido de una línea en blanco y, a continuación, del cuerpo del correo electrónico. El sobre no se muestra, ya que se comunica entre el cliente y el servidor de email durante la sesión de SMTP, en lugar de una parte del propio email.

```
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
```

En las secciones siguientes se revisan los encabezados y los cuerpos de los mensajes de correo electrónico y se identifica la información que tiene que proporcionar cuando utilice Amazon SES.

Encabezado de correo electrónico

Hay un encabezado por mensaje de correo electrónico. Cada línea del encabezado contiene un campo seguido de dos puntos seguidos del cuerpo de campo. Al leer un correo electrónico en un cliente de correo electrónico, el cliente de correo electrónico normalmente muestra los valores de los siguientes campos de encabezado:

- To: las direcciones de correo electrónico de los destinatarios del mensaje.
- CC: las direcciones de correo electrónico de los destinatarios de copia del mensaje.
- From: la dirección de correo electrónico desde la que se envía el correo electrónico.

- Subject: un resumen del tema del mensaje.
- Date: la hora y la fecha en la que se envía el correo electrónico.

Existen muchos campos de encabezado adicionales que proporcionan información de enrutamiento y describen el contenido del mensaje. Los clientes de correo electrónico habituales no suelen mostrar estos campos al usuario. Para obtener una lista completa de los campos de encabezado que acepta Amazon SES, consulte Campos de encabezado de Amazon SES. Cuando utiliza Amazon SES, necesita especialmente conocer la diferencia entre los campos de encabezado “From”, “Reply-To” y “Return-Path”. Como se ha indicado anteriormente, la dirección de remitente ("From") es la dirección de correo electrónico del remitente del correo electrónico, mientras que "Reply-To" y "Return-Path" son lo siguiente:

- Reply-To: dirección de correo electrónico a la que se enviarán las respuestas. De forma predeterminada, las respuestas se envían a la dirección de correo electrónico del remitente original.
- Return-Path: dirección de correo electrónico a la que se deben enviar los rebotes y reclamos. "Return-Path" se denomina en ocasiones "envelope from", "envelope sender" o "MAIL FROM".

> **Note**
>
> Cuando utiliza Amazon SES, le recomendamos que defina siempre el parámetro “Return-Path” para que pueda estar al tanto de los rebotes y tomar medidas correctivas si se producen.

Para asignar con facilidad un mensaje rebotado a su destinatario deseado, puede usar la ruta variable de retorno de sobres (VERP). Con VERP, se define una "Return-Path" distinta para cada destinatario, de modo que si el mensaje rebota, se sabe automáticamente qué destinatario lo ha rebotado, en lugar de tener que abrir el mensaje de rebote y analizarlo.

Cuerpo de correo electrónico

El cuerpo del correo electrónico contiene el texto del mensaje. El cuerpo se puede enviar en los siguientes formatos:

- HTML: si el cliente de correo electrónico del destinatario puede interpretar HTML, el cuerpo puede incluir texto con formato y enlaces de hipertexto.

- Texto sin formato: si el cliente de correo electrónico del destinatario es de texto, el cuerpo no debe contener caracteres no imprimibles.
- Tanto HTML como texto sin formato: cuando utiliza ambos formatos para enviar el mismo contenido en un único mensaje, el cliente de correo electrónico del destinatario decide qué mostrar, en función de sus capacidades.

Si envía un mensaje de correo electrónico a un gran número de destinatarios, es razonable enviarlo tanto en HTML como en texto. Algunos destinatarios tendrán clientes de correo electrónico compatibles con HTML, de forma que puedan hacer clic en los enlaces incorporados en el mensaje. Los destinatarios que utilizan clientes de correo electrónico de texto tendrán que incluir direcciones URL que puedan copiar y abrir mediante un navegador web.

Información de correo electrónico que tiene que proporcionar a Amazon SES

Cuando envíe un correo electrónico con Amazon SES, la información de este que debe proporcionar depende de cómo llame a Amazon SES. Puede proporcionar un nivel mínimo de información y hacer que Amazon SES se ocupe de todo el formato. O, si desea hacer algo más avanzado, como enviar un archivo adjunto, puede proporcionar el mensaje sin procesar usted mismo. En las secciones siguientes, se revisa qué tiene que proporcionar cuando envíe un correo electrónico a través de la API de Amazon SES, la interfaz de SMTP de Amazon SES o la consola de Amazon SES.

API de Amazon SES

Si llama a la API de Amazon SES directamente, llame a la API `SendEmail`, o bien `SendRawEmail`. La cantidad de información que tiene que proporcionar depende de la API que se llame.

- `SendEmail API` requiere que el usuario proporcione únicamente una dirección de origen, una dirección de destino, un asunto del mensaje y un cuerpo del mensaje. Si lo desea, puede proporcionar las direcciones "Reply-To". Cuando llama a esta API, Amazon SES crea automáticamente un mensaje de correo electrónico Multipurpose Internet Mail Extensions (MIME) con formato multiparte optimizado para su visualización en el software de cliente de correo electrónico. Para obtener más información, consulte Envío de correo electrónico con formato mediante la API de Amazon SES .
- La API `SendRawEmail` le ofrece flexibilidad para dar formato y enviar sus propios emails sin procesar mediante la especificación de los encabezados, las partes de MIME y los tipos de contenido. La API `SendRawEmail` suelen utilizarla los usuarios avanzados. Tiene que proporcionar el cuerpo del mensaje y todos los campos de encabezado que se especifican como

obligatorios en la especificación de formato de mensajes de Internet (RFC 5322). Para obtener más información, consulte Envío de correo electrónico sin procesar mediante la API v2 de Amazon SES .

Si utiliza un SDK de AWS para llamar a la API de Amazon SES, proporcione la información indicada más arriba a las funciones correspondientes (por ejemplo, `SendEmail` y `SendRawEmail` para Java).

Para obtener más información acerca del envío de correo electrónico mediante la API de Amazon SES, consulte Uso de la API de Amazon SES para enviar correo electrónico.

Interfaz de SMTP de Amazon SES

Cuando acceda a Amazon SES a través de la interfaz de SMTP, su aplicación cliente de SMTP crea el mensaje, de modo que la información que necesita proporcionar depende de la aplicación que esté utilizando. Como mínimo, el intercambio SMTP entre un cliente y un servidor requiere una dirección de origen, una dirección de destino y datos de mensaje.

Para obtener más información acerca del envío de correo electrónico mediante la interfaz SMTP de Amazon SES, consulte Uso de la interfaz de SMTP de Amazon SES para enviar correo electrónico.

Consola de Amazon SES

Cuando envíe un correo electrónico a través de la consola de Amazon SES, la cantidad de información que tiene que proporcionar depende de si opta por enviar un correo electrónico sin procesar o con formato.

- Para enviar un correo electrónico con formato, tiene que proporcionar una dirección de origen, una dirección de destino, un asunto del mensaje y un cuerpo del mensaje. Amazon SES crea automáticamente un mensaje de correo electrónico MIME con formato multiparte optimizado para su visualización por el software de cliente del correo electrónico. También puede especificar un campo Reply-To y Return-Path.
- Para enviar un mensaje de correo electrónico sin procesar, proporcione la dirección de origen, una dirección de destino y el contenido del mensaje, que debe contener el cuerpo del mensaje y todos los campos de encabezado que se especifican como obligatorios en la especificación de formato de mensajes de Internet (RFC 5322).

Descripción de la capacidad de entrega de correo electrónico en Amazon SES

Desea que sus destinatarios lean sus correos electrónicos, los encuentren útiles y no los etiqueten como spam. En otras palabras, desea mejorar la capacidad de entrega del correo electrónico: el porcentaje de sus correos electrónicos que llega a las bandejas de entrada de los destinatarios. Este tema revisa conceptos de capacidad de entrega de correo electrónico que debe conocer cuando utilice Amazon SES.

Para mejorar la capacidad de entrega de correo electrónico, necesita conocer los problemas de entrega de correo electrónico, tomar medidas de forma proactiva para evitarlos, mantenerse informado acerca del estado de los mensajes de correo electrónico que envíe y, además, mejorar el programa de envío de correo electrónico, si es necesario, para aumentar aún más la probabilidad de éxito de las entregas. En las secciones siguientes se revisan los conceptos subyacentes a estos pasos y cómo Amazon SES lo ayuda a realizar el proceso.

Entender los problemas de entrega de correo electrónico

En la mayoría de los casos, los mensajes se envían de forma correcta a los destinatarios que los esperan. En algunos casos, sin embargo, una entrega podría devolver un error o un destinatario podría no desea recibir el correo que está enviando. Los rebotes, las reclamaciones y la lista de supresión están relacionados con estos problemas de entrega y se describen en las siguientes secciones.

Bounce (Rebotar)

Si el receptor de su destinatario (por ejemplo, un proveedor de correo electrónico) no consigue entregar el mensaje al destinatario, el receptor rebota el mensaje y lo envía a Amazon SES. Amazon SES lo notifica seguidamente acerca de los mensajes de correo electrónico rebotados por correo electrónico o a través de Amazon Simple Notification Service (Amazon SNS), en función de cómo haya configurado el sistema. Para obtener más información, consulte Configuración de las notificaciones de eventos para Amazon SES .

Hay rechazos permanentes y rebotes temporales, como se indica a continuación:

- Rechazo permanente: error permanente de entrega de correo electrónico. Por ejemplo, el buzón de correo no existe. Amazon SES no reintentará los rechazos permanentes, con la excepción de los errores de búsqueda de DNS. Le recomendamos encarecidamente que no realice intentos de entrega repetidos a las direcciones de correo electrónico que presentan rebote permanente.
- Rebote temporal: error temporal de entrega de correo electrónico. Por ejemplo, el buzón de correo está lleno, hay demasiadas conexiones (también denominado limitación controlada) o se agota el tiempo de espera de la conexión. Amazon SES vuelve a intentar los rebotes temporales varias veces. Si el correo electrónico todavía no se puede enviar, Amazon SES deja de reintentarlo.

Amazon SES le notifica acerca de los rebotes permanentes y los rebotes temporales que ya no se volverán a intentar. Sin embargo, solo los rechazos permanentes se tienen en cuenta en la tasa de rebotes y la métrica de rebotes que se recupera a través de la consola de Amazon SES o la API `GetSendStatistics`.

Los rebotes además pueden ser síncronos o asíncronos. Un rebote síncrono se produce mientras los servidores de correo electrónico del remitente y del receptor se están comunicando de forma activa. Un rebote asíncrono que se produce cuando un receptor acepta inicialmente un mensaje de correo electrónico para su entrega y posteriormente no consigue entregarlo al destinatario.

Complaint

La mayoría de los programas cliente de correo electrónico ofrecen un botón "Marcar como spam", o similar, que traslada el mensaje a una carpeta de spam y lo reenvía al proveedor de correo electrónico. Además, la mayoría de los proveedores de correo electrónico mantienen una dirección de abuso (por ejemplo, abuse@example.net), donde los usuarios pueden reenviar mensajes de correo electrónico no deseados y solicitar al proveedor de correo electrónico que tome las medidas necesarias para evitarlos. En ambos casos, el destinatario está realizando una reclamación. Si el proveedor de correo electrónico concluye que usted es un spammer y Amazon SES tiene un bucle de retroalimentación configurado con el proveedor de correo electrónico, el proveedor de correo electrónico enviará el reclamo de nuevo a Amazon SES. Cuando Amazon SES reciba un reclamo de este tipo, se lo reenviará a usted por correo electrónico o mediante una notificación de Amazon SNS, en función de cómo tenga configurado el sistema. Para obtener más información, consulte Configuración de las notificaciones de eventos para Amazon SES . Le recomendamos encarecidamente que no realice intentos de entrega repetidos a las direcciones de correo electrónico que generen reclamaciones.

Lista de supresión global

La lista de supresión global de Amazon SES, propiedad y administración a cargo de SES que tiene como objetivo proteger la reputación de las direcciones del grupo de IP compartidas de SES, contiene direcciones de correo electrónico de destinatarios que recientemente han provocado un rechazo permanente para cualquier cliente de SES. Si intenta enviar un correo electrónico a través de SES a una dirección incluida en la lista de supresión, la llamada a SES tendrá se realizará correctamente, pero SES tratará el correo como un rechazo permanente en lugar de intentar enviarlo. Al igual que con el rebote permanente, las devoluciones de la lista de supresión se tienen en cuenta en la cuota de envío y en la tasa de rebotes. Una dirección de correo electrónico puede permanecer en la lista de supresión durante un periodo máximo de 14 días. Si está seguro de que la dirección de correo electrónico a la que está intentando enviar el correo es válida, puede anular la lista de supresión global y asegurarse de que la dirección no aparezca en su lista de supresión a nivel de cuenta. SES intentará efectuar la entrega, pero si rebota, el rebote afectará su propia reputación, aunque nadie recibirá rebotes porque no pueden enviar a esa dirección de correo electrónico si no están utilizando su propia lista de supresión a nivel de cuenta. Para comprender mejor la lista de supresión a nivel de cuenta, consulte Uso de la lista de supresión de nivel de cuenta de Amazon SES.

Ser proactivo

Uno de los principales problemas del correo electrónico en Internet es el correo masivo no solicitado o spam. Los proveedores de correo electrónico adoptan muchas medidas para impedir que sus clientes reciban spam. Amazon SES también toma medidas para reducir la probabilidad de que los proveedores de correo electrónico consideren sus mensajes de correo electrónico como spam. Amazon SES utiliza la verificación, la autenticación, las cuotas de envío y el filtrado de contenido. Amazon SES también mantiene una reputación de confianza con los proveedores de servicios de Internet y exige que envíe mensajes de correo electrónico de alta calidad. Amazon SES realiza algunas de estas cosas automáticamente (como el filtrado de contenidos); en otros casos, facilita las herramientas (como la autenticación) o lo guía en la dirección correcta (cuotas de envío). Las siguientes secciones brindan más información sobre cada concepto.

Verification (Verificación)

Desgraciadamente, un spammer podría falsificar un encabezado de correo electrónico y suplantar la dirección de correo electrónico de origen para aparentar que el correo electrónico procede de una fuente diferente. Para mantener la confianza entre los proveedores de correo electrónico y Amazon SES, Amazon SES tiene que asegurarse de que los remitentes son quienes dicen ser. Por lo tanto, es necesario que verifique todas las direcciones de correo electrónico desde las que envía mensajes de correo electrónico a través de Amazon SES para proteger su identidad de envío. Puede verificar las direcciones de correo electrónico mediante la consola de Amazon SES o con la API de Amazon SES. También puede verificar dominios completos. Para obtener más información, consulte Creación de una identidad de dirección de correo electrónico y Creación de una identidad de dominio.

Si la cuenta sigue estando en el entorno de pruebas de Amazon SES, también deberá verificar todas las direcciones de los destinatarios, excepto las direcciones proporcionadas por el simulador de buzón de correo de Amazon SES. Para obtener información sobre cómo salir del entorno de pruebas, consulte Solicitar acceso a la producción (salir del entorno de pruebas de Amazon SES). Para obtener más información sobre el simulador de bandeja de correo, consulte Uso del simulador de buzón de correo de forma manual.

Autenticación

La autenticación es otra forma en que puede indicar a los proveedores de correo electrónico que es quien dice ser. Para autenticar un correo electrónico, deberá aportar una prueba de que es el dueño de la cuenta y sus emails no se han modificado en tránsito. En algunos casos, los proveedores de correo electrónico rechazan reenviar correo electrónico que no está autenticado. Amazon SES admite dos métodos de autenticación: el marco de políticas de remitentes (SPF) y el correo

identificado con claves de dominio (DKIM). Para obtener más información, consulte Configuración de identidades en Amazon SES .

Cuotas de envío

Si un proveedor de correo electrónico detecta picos repentinos e inesperados en el volumen o en la frecuencia de sus correos electrónicos, el proveedor podría sospechar que se trata de un spammer y bloquear los mensajes de correo electrónico. Por lo tanto, cada cuenta de Amazon SES tiene un conjunto de cuotas de envío. Estas cuotas restringen el número de correos electrónicos que puede enviar en un período de 24 horas y el número que puede enviar por segundo. Estas cuotas de envío ayudan a proteger su confianza con los proveedores de correo electrónico.

En la mayoría de los casos, si es un usuario nuevo, Amazon SES le permite enviar una pequeña cantidad de correo electrónico cada día. Si el correo que envía es aceptable para los proveedores de correo electrónico, aumentaremos automáticamente esta cuota. Con el paso del tiempo, las cuotas de envío aumentarán de forma constante para que pueda enviar grandes cantidades de correo electrónico con mayor frecuencia. También puede crear un caso de aumento de límites de envío de SES para solicitar aumentos adicionales en las cuotas.

Para obtener más información sobre las cuotas de envío y cómo aumentarlas, consulte Administración de sus límites de envío de Amazon SES.

Filtrado de contenido

Muchos proveedores de correo electrónico utilizan el filtrado de contenido para determinar si los correos electrónicos entrantes son spam. Los filtros de contenido buscan contenidos dudosos y bloquean el correo electrónico si el correo electrónico encaja en el perfil de spam. Amazon SES utiliza también filtros de contenido. Cuando la aplicación envía una solicitud a Amazon SES, Amazon SES crea un mensaje de correo electrónico en su nombre y, a continuación, analiza el encabezado y el cuerpo del mensaje para determinar si incluyen contenido que los proveedores de correo electrónico puedan interpretar como spam. Si los mensajes parecen spam para los filtros de contenido que utiliza Amazon SES, su reputación con Amazon SES se verá afectada negativamente.

Amazon SES también analiza todos los mensajes para detectar la presencia de virus. Si un mensaje contiene un virus, Amazon SES no intenta entregarlo al servidor de correo electrónico del destinatario.

Reputación

En lo referente al envío de correo electrónico, la reputación (que mide la confianza en que una dirección IP, dirección de correo electrónico o dominio remitente no constituye una fuente de

spam) es importante. Amazon SES mantiene una gran reputación con los proveedores de correo electrónico, de forma que entreguen su correo electrónico a las bandejas de entrada de sus destinatarios. Del mismo modo, debe mantener una reputación de confianza con Amazon SES. La reputación se crea en Amazon SES cuando se envía contenido de alta calidad. Al enviar contenido de alta calidad, su reputación pasa a ser de mayor confianza con el tiempo y Amazon SES aumenta sus cuotas de envío. Los rebotes y reclamos excesivos afectan negativamente a su reputación y pueden hacer que Amazon SES reduzca las cuotas de envío de su cuenta o que se termine su cuenta de Amazon SES.

Una forma de ayudar a mantener su reputación consiste en utilizar el simulador de bandeja de correo al probar su sistema, en lugar de enviar a las direcciones de correo electrónico que haya creado usted mismo. Los correos electrónicos enviados al simulador de bandeja de correo no cuentan para la métrica de rebotes y reclamaciones. Para obtener más información sobre el simulador de bandeja de correo, consulte Uso del simulador de buzón de correo de forma manual.

Correo electrónico de alta calidad

El correo electrónico de alta calidad es aquel que los destinatarios consideran valioso y desean recibir. El significado de “valioso” varía en función de cada destinatario y puede referirse a ofertas, confirmaciones de pedidos, recibos, boletines informativos, etc. En última instancia, su capacidad de entrega se basa en la calidad de los mensajes de correo electrónico que envíe, dado que los proveedores de correo electrónico bloquean los correos electrónicos que consideran de baja calidad.

Mantenerse informado

Tanto si las entregas no se realizan correctamente, como si los destinatarios se quejan de sus mensajes de correo electrónico o Amazon SES entrega correctamente un correo electrónico al servidor de correo electrónico de un destinatario, Amazon SES lo ayuda a localizar el problema mediante notificaciones y le permite monitorear con facilidad las estadísticas de uso.

Notificaciones

Cuando un correo electrónico rebota, el proveedor de correo electrónico notifica a Amazon SES y Amazon SES se lo notifica a usted. Amazon SES le notifica acerca de los rechazos permanentes y los rebotes temporales que ya no volverá a intentar. Muchos proveedores de correo electrónico también reenvían reclamos, y Amazon SES configura bucles de retroalimentación de reclamos con los principales proveedores de correo electrónico para que no tenga que hacerlo. Amazon SES puede notificarle de rebotes, reclamos y entregas correctas de dos formas: mediante la configuración de su cuenta para recibir notificaciones a través de Amazon SNS o la recepción de notificaciones por

correo electrónico (solo rebotes y reclamos). Para obtener más información, consulte Configuración de las notificaciones de eventos para Amazon SES .

Estadísticas de uso

Amazon SES ofrece estadísticas de uso para que pueda ver las entregas con error para determinar y resolver las causas. Puede ver sus estadísticas de uso mediante la consola de Amazon SES o con la API de Amazon SES. Puede ver cuántas entregas, rebotes, reclamaciones y correos electrónicos rechazados infectados por virus tiene y también puede consultar las cuotas de envío para asegurarse de no rebasarlas.

Mejorar su programa de envío de correo electrónico

Si obtiene un gran número de rebotes y reclamaciones, es hora de replantearse su estrategia de envío de correos electrónicos. Recuerde que un número excesivo de rebotes, reclamos e intentos de enviar correo de baja calidad supondrán abuso y supondrán un riesgo de que se cierre su Cuenta de AWS. En definitiva, debe asegurarse de que utiliza Amazon SES para enviar mensajes de correo electrónico de alta calidad únicamente a los destinatarios que desean recibirlos.

Al menos una entrega

Amazon SES almacena copias de los mensajes en varios servidores para mejorar la redundancia y lograr una alta disponibilidad. En raras ocasiones, uno de los servidores que almacena una copia de un mensaje podría no estar disponible cuando usted reciba o elimine un mensaje.

En este caso, la copia no se elimina en el servidor no disponible y podría recibir una nueva copia al recibir mensajes. Diseñe sus aplicaciones de modo que sean idempotentes (no deben verse afectadas negativamente si se procesa el mismo mensaje más de una vez).

Prácticas recomendadas para el envío de correo electrónico utilizando Amazon SES

El modo en que gestione sus comunicaciones por correo electrónico con los clientes se denomina programa de correo electrónico. Hay varios factores que pueden dar lugar al éxito o al fracaso de su programa de correo electrónico; estos factores puede resultar confusos o misteriosos al principio. Sin embargo, si entiende cómo se entrega de correo electrónico y sigue algunas prácticas recomendadas, puede aumentar las probabilidades de que su correo electrónico llegue con éxito a las bandejas de entrada de sus clientes.

Temas

- Métricas de éxito para los programas de correo electrónico
- Consejos y prácticas recomendadas

Métricas de éxito para los programas de correo electrónico

Existen varias métricas que pueden ayudarle a medir el éxito de su programa de correo electrónico.

Esta sección ofrece información sobre los siguientes temas:

- Rebotes
- Reclamos
- Calidad del mensaje

Rebotes

Un rebote se produce cuando un correo electrónico no se puede entregar al destinatario esperado. Existen dos tipos de rebotes: rebotes permanentes y rebotes temporales. Un rebote permanente se produce cuando el correo electrónico no se puede entregar debido a un problema persistente, como, por ejemplo, cuando no existe la dirección de correo electrónico. Un rebote temporal se produce cuando un problema temporal impide la entrega de un mensaje de correo electrónico. Los rebotes temporales pueden producirse cuando la bandeja de entrada de un destinatario está llena o cuando el servidor de recepción no está disponible temporalmente. Amazon SES gestiona los rebotes temporales intentando volver a enviar mensajes de correo electrónico con rebote temporal durante un determinado periodo de tiempo.

Es fundamental que monitorice el número de rebotes permanentes en su programa de correo electrónico y que retire las direcciones de correo electrónico con rebotes permanentes de su lista de destinatarios. Cuando los receptores de correo electrónico detectan una alta tasa de rebotes permanentes, suponemos que no conoce a sus destinatarios bien. En consecuencia, una tasa de rebotes permanentes elevada puede afectar negativamente a la capacidad de entrega de sus mensajes de correo electrónico.

Las siguientes directrices le pueden ayudar a evitar los rebotes y a mejorar su reputación de remitente:

- Intente mantener su tasa de rebotes permanentes por debajo del 5 %. Mientras menor sea el número de rebotes permanentes en su programa de correo electrónico, más probable será que

los ISP vean sus mensajes como legítimos y valiosos. Esta tasa debería considerarse un objetivo razonable y alcanzable, pero no es una regla universal en todos los proveedores de Internet.

- No alquile ni compre nunca listas de direcciones de correo electrónico. Estas listas pueden contener un gran número de direcciones no válidas, lo que podría hacer que sus tasas de rebotes permanentes aumenten de manera notable. Además, estas listas podrían contener trampas de spam: direcciones de correo electrónico utilizadas específicamente para capturar remitentes ilegítimos. Si sus mensajes caen en una trampa de spam, sus tasas de envío y su reputación de remitente podría verse perjudicadas de manera irrevocable.
- Mantenga la lista actualizada. Si no ha enviado correo electrónico a sus destinatarios desde hace mucho tiempo, pruebe a validar los estados de sus clientes a través de algún otro medio (por ejemplo, la actividad de inicio de sesión del sitio web o historial de compras).
- Si no dispone de un método de verificación de los estados de sus clientes, considere la posibilidad de enviar una correo electrónico de recuperación. Un correo electrónico de recuperación normal indica que no ha tenido noticias del cliente desde hace tiempo y anima al cliente a confirmar que todavía desea recibir su correo electrónico. Después de enviar correo electrónico de recuperación, elimine a todos los destinatarios que no hayan respondido a partir de sus listas.

Cuando reciba rebotes, es fundamental que responda a ellos de forma adecuada respetando las reglas siguientes:

- Si una dirección de correo electrónico presenta rebotes permanentes, elimine de inmediato esa dirección de sus listas. No intente volver a enviar mensajes a direcciones con rebotes permanentes. Los rebotes permanentes repetidos se acumulan y, en última instancia, dañan su reputación en el ISP del destinatario.
- Asegúrese de que la dirección que utiliza para recibir las notificaciones de rebote sea capaz de recibir correo electrónico. Para obtener más información acerca de la configuración de notificaciones de rebotes y reclamos, consulte Configuración de las notificaciones de eventos para Amazon SES.
- Si su correo electrónico entrante le llega desde un ISP, en lugar de a través de sus propios servidores internos, un flujo de las notificaciones de rebote puede acabar en su carpeta de spam o se puede eliminar por completo. Idealmente, no debe utilizar una dirección de correo electrónico alojada para recibir rebotes. Si es necesario, sin embargo, compruebe la carpeta de spam a menudo y no marque los mensajes de rebotes como spam. En Amazon SES, puede especificar la dirección a la que se envían las notificaciones de rebote.

- Normalmente, un rebote proporciona la dirección del buzón que rechaza la entrega. Sin embargo, si necesita datos más detallados para asignar la dirección de un destinatario a una determinada campaña de correo electrónico, incluya un encabezado X con un valor del que pueda realizar un seguimiento en su sistema de seguimiento interno. Para obtener más información, consulte Campos de encabezado de Amazon SES.

Reclamos

Una reclamación se produce cuando un destinatario de correo electrónico hace clic en el botón "Marcar como spam" (o equivalente) en su cliente de correo electrónico basado en web. Si acumula un gran número de estas reclamaciones, el ISP supone que está enviando spam. Esto tiene un impacto negativo en su tasa de capacidad de entrega y en su reputación de remitente. Algunos de los proveedores de servicios de Internet, aunque no todos, le avisarán cuando se notifique un reclamo; esto se conoce como un bucle de retroalimentación. Amazon SES le reenvía automáticamente los reclamos de los ISP que ofrecen bucles de retroalimentación.

Las siguientes directrices le puede ayudar a evitar las reclamaciones y a mejorar su reputación de remitente:

- Intente mantener su tasa de reclamaciones por debajo del 0,1 %. Mientras menor sea el número de reclamaciones en su programa de correo electrónico, más probable será que los ISP vean sus mensajes como legítimos y valiosos. Esta tasa debería considerarse un objetivo razonable y alcanzable, pero no es una regla universal en todos los proveedores de Internet.
- Si un cliente se queja de un correo electrónico de marketing, debe dejar de enviar inmediatamente correos electrónicos de marketing a dicho cliente. Sin embargo, si su programa de correo electrónico también incluye otros tipos de correos electrónicos (como, por ejemplo, correos electrónicos de notificaciones o transaccionales), puede ser aceptable seguir enviando estos tipos de mensajes al destinatario que realizó la reclamación.
- Al igual que ocurre con los rebotes permanentes, si dispone de una lista a la que no haya enviado correo electrónico desde hace algún tiempo, asegúrese de que sus destinatarios entiendan por qué están recibiendo sus mensajes. Le recomendamos que envíe un mensaje de bienvenida que les recuerde quién es usted y por qué desea ponerse en contacto con ellos.

Cuando reciba las reclamaciones, es fundamental que responda a las mismas de forma adecuada respetando las reglas siguientes:

- Asegúrese de que la dirección que utiliza para recibir las notificaciones de reclamación sea capaz de recibir correo electrónico. Para obtener más información acerca de la configuración de notificaciones de rebotes y reclamos, consulte Configuración de las notificaciones de eventos para Amazon SES.
- Asegúrese de que sus notificaciones de reclamación no la marque como spam su ISP o sistema de correo electrónico.
- Las notificaciones de reclamaciones suelen contener el cuerpo del correo electrónico; esto es diferente de las notificaciones de rebote, que solo incluyen los encabezados de correo electrónico. Sin embargo, en las notificaciones de reclamaciones, se quita la dirección de correo electrónico de la persona que formuló la reclamación. Utilice los encabezados X personalizados o identificadores especiales incrustados en el cuerpo de correo electrónico para que pueda identificar la dirección de correo electrónico que presentó la reclamación. Esta técnica facilita identificar las direcciones que reclamaron para que pueda eliminarlas de su lista de destinatarios.

Calidad del mensaje

Los receptores de correo electrónico utilizan filtros de contenido para detectar determinados atributos en sus mensajes para identificar si su mensaje es legítimo. Estos filtros de contenido revisan automáticamente el contenido de sus mensajes para identificar características comunes de mensajes no deseados o malintencionados. Amazon SES utiliza tecnologías de filtrado de contenido que ayudan a detectar y bloquear los mensajes que contienen malware antes de que se envíen.

Si los filtros de contenido de un receptor de correo electrónico determinan que su mensaje contiene las características de spam o correo electrónico malintencionado, su mensaje probablemente marcará y desviará de las bandejas de entrada de los destinatarios.

Recuerde lo siguiente a la hora de diseñar su correo electrónico:

- Los filtros de contenido modernos son inteligentes, se adaptan y cambian de forma continua. No se basan en un conjunto de reglas predefinidas. Los servicios de terceros como ReturnPath o Litmus pueden ayudar a identificar contenido en su correo electrónico que podría activar los filtros de contenido.
- Si el correo electrónico contiene enlaces, verifique las direcciones URL de dichos enlaces en listas de agujero negro basadas en DNS (DNSBL), como las que se encuentran en URIBL.com y SURBL.org.
- Evite el uso de acortadores de enlaces. Los remitentes malintencionados podrían utilizar los acortadores de enlaces para ocultar el destino real de un enlace. Si los ISP observan que se

utilizan con fines perversos los servicios de acortamiento de enlaces, incluso los más reputados, podrían denegar el acceso a dichos servicios también. Si su correo electrónico contiene un enlace a un servicio acortador de enlace que se ha agregado a una lista de denegación, no llegará a las bandejas de entrada de sus clientes y el éxito de su campaña de correo electrónico se resentirá.

- Pruebe cada enlace de su correo electrónico para asegurarse de que apunte a la página deseada.
- Asegúrese de que su sitio web incluya los documentos de Política de privacidad y Términos de uso y que dichos documentos estén actualizados. Es una buena práctica enlazar a estos documentos de cada mensaje de correo electrónico que envíe. Proporcionar enlaces a estos documentos demuestra que no tiene nada que ocultar a sus clientes, lo que pueden contribuir a forjar una relación de confianza.
- Si tiene previsto enviar contenido con mucha frecuencia (como, por ejemplo, mensajes con "ofertas diarias"), asegúrese de que el contenido de su correo electrónico sea diferente en cada implementación. Al enviar mensajes con mucha frecuencia, debe asegurarse de que los mensajes sean oportunos y relevantes, en lugar de repetitivos y molestos.

Consejos y prácticas recomendadas

Incluso cuando tenga en cuenta el mayor interés para sus clientes, es posible que encuentre situaciones que afecten a la capacidad de entrega de sus mensajes. Las siguientes secciones contienen recomendaciones para ayudarle a garantizar que sus comunicaciones por correo electrónico lleguen a la audiencia deseada.

Recomendaciones generales

- Póngase en el lugar del cliente. Plantéese si el mensaje que está enviando es algo que desearía recibir en su propia bandeja de entrada. Si la respuesta no es un “¡sí!” entusiasta, probablemente no debería enviarlo.
- Algunos sectores tiene una reputación de mala calidad o incluso de prácticas de correo electrónico malintencionadas. Si participa en los siguientes sectores, debe monitorizar su reputación con atención y resolver los problemas de forma inmediata:
  - Hipotecas domésticas
  - Créditos
  - Productos farmacéuticos y suplementos
  - Alcohol y tabaco
  - Ocio para adultos

- Casinos y juegos de azar
- Programas de trabajo desde casa

Consideraciones sobre dominios y direcciones de remitente ("from")

- Piense detenidamente sobre las direcciones desde las que envía correo electrónico. La dirección de remitente ("From") es uno de los primeros elementos de información que ven sus destinatarios y, por lo tanto, pueden dejar una primera impresión duradera. Además, algunos proveedores de Internet asocian su reputación con su dirección de remitente ("From").
- Considere la posibilidad de utilizar subdominios para los distintos tipos de las comunicaciones. Por ejemplo, suponga que va a enviar correo electrónico desde el dominio example.com y que desea enviar tanto mensajes de marketing como de transacciones. En lugar de enviar todos sus mensajes desde example.com, envíe sus mensajes de marketing desde un subdominio como marketing.example.com y sus mensajes de transacciones desde un subdominio como orders.example.com. Los subdominios únicos desarrollan sus propias reputaciones. El uso de subdominios reduce el riesgo de dañar su reputación si, por ejemplo, las comunicaciones de marketing caen en una trampa de spam o activan un filtro de contenido.
- Si tiene previsto enviar un gran número de mensajes, no envíe los mensajes desde una dirección basada en ISP como, por ejemplo, sender@hotmail.com. Si un ISP observa un gran volumen de mensajes de correo electrónico procedentes de sender@hotmail.com, dicho correo electrónico se trata de manera distinta a un correo electrónico que provenga de un dominio de envío de correo electrónico saliente de su propiedad.
- Trabaje con su registro de dominios para garantizar que la información WHOIS de su dominio sea correcta. Mantener un registro de WHOIS honrado y actualizado demuestra que valora la transparencia y permite a los usuarios identificar rápidamente si su dominio es legítimo o no.
- Evite utilizar dirección no-reply como, por ejemplo, no-reply@example.com, como dirección de remitente ("From") o de respuesta ("Reply-to"). Utilizando una dirección de correo electrónico no-reply@ envía a sus destinatarios un mensaje claro: que no les está ofreciendo una forma de ponerse en contacto con usted y que no le interesan sus comentarios.

Autenticación

- Autentique su dominio con SPF y SenderID. Estos métodos de autenticación confirman a los destinatarios de correo electrónico que cada correo electrónico que envía procede realmente del dominio que dice proceder.

- Firme su correo electrónico saliente con DKIM. Este paso confirma a los destinatarios que el contenido no se ha cambiado en tránsito entre el emisor y el receptor.
- Puede probar su configuración de autenticación para SPF y DKIM enviando un correo electrónico a una dirección de correo electrónico basada en ISP que posea, como, por ejemplo, una cuenta personal de Gmail o Hotmail y, a continuación, visualizar los encabezados del mensaje. Los encabezados indican si sus intentos de autenticar y firmar el mensaje se han realizado correctamente.

Creación y mantenimiento de sus listas

- Aplicar un doble estrategia de confirmación. Cuando los usuarios se registren para recibir su correo electrónico, envíeles un mensaje con un enlace de confirmación y no empiece a enviarles correo electrónico hasta que confirmen su dirección de correo electrónico haciendo clic en el enlace. Una estrategia de confirmación doble ayuda a reducir el número de rebotes permanente derivados de errores tipográficos.
- Al recopilar las direcciones de correo electrónico con un formulario basado en web, lleve a cabo una validación mínima en estas direcciones de envío una vez enviadas. Por ejemplo, asegúrese de que las direcciones que recopila estén bien formadas (es decir, que se encuentran en el formato recipient@example.com) y que hacen referencia a dominios con registros MX válidos.
- Tenga cuidado al permitir que una entrada definida por el usuario se transfiera a Amazon SES sin comprobar. Los registros en foros y los envíos de formularios presentan riesgos únicos, ya que el contenido está completamente generado por el usuario y los spammers pueden rellenar formularios con su propio contenido. Es responsabilidad suya asegurarse de que solo envía correo electrónico con contenido de alta calidad.
- Es muy improbable que un alias estándar (por ejemplo, postmaster@, abuse@ o noc@) se suscriba a su correo electrónico de forma intencionada. Asegúrese de que solo envía mensajes a personas reales que realmente desean recibirlos. Esta regla se da especialmente en el caso de alias estándar, que se reservan habitualmente para guardianes de correo electrónico. Estos alias se pueden añadir de forma malintencionada a su lista como forma de sabotaje, a fin de dañar la reputación.

Conformidad de

- Tenga en cuenta de los reglamentos y de la legislación antispam y de marketing de correo electrónico en los países y regiones donde envía correo electrónico. Es usted responsable de garantizar que el correo electrónico que envía cumpla con estas leyes. En esta guía no se explican

estas leyes, por lo que es importante que las investigue. Para obtener un listado de leyes, consulte Email Spam Legislation by Country en Wikipedia.

- Consulte siempre a un abogado para obtener asesoramiento jurídico.

Uso de Amazon SES con un AWS SDK

AWS Los kits de desarrollo de software (SDK) están disponibles para muchos lenguajes de programación populares. Cada SDK proporciona una API, ejemplos de código y documentación que facilitan a los desarrolladores la creación de aplicaciones en su lenguaje preferido.

Documentación de SDK	Ejemplos de código
AWS SDK for C++	AWS SDK for C++ ejemplos de código
AWS CLI	AWS CLI ejemplos de código
AWS SDK for Go	AWS SDK for Go ejemplos de código
AWS SDK for Java	AWS SDK for Java ejemplos de código
AWS SDK for JavaScript	AWS SDK for JavaScript ejemplos de código
AWS SDK para Kotlin	AWS SDK para Kotlin ejemplos de código
AWS SDK for .NET	AWS SDK for .NET ejemplos de código
AWS SDK for PHP	AWS SDK for PHP ejemplos de código
AWS Tools for PowerShell	Herramientas para ejemplos PowerShell de código
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) ejemplos de código
AWS SDK for Ruby	AWS SDK for Ruby ejemplos de código
AWS SDK para Rust	AWS SDK para Rust ejemplos de código
AWS SDK para SAP ABAP	AWS SDK para SAP ABAP ejemplos de código

Documentación de SDK	Ejemplos de código
AWS SDK para Swift	AWS SDK para Swift ejemplos de código

Para obtener ejemplos específicos de Amazon SES, consulte Ejemplos de código de Amazon SES con SDK de AWS.

> **Ejemplo de disponibilidad**
>
> ¿No encuentra lo que necesita? Solicite un ejemplo de código a través del enlace de Enviar comentarios que se encuentra al final de esta página.

Introducción a Amazon Simple Email Service

Este capítulo le guía a través de las tareas que debe realizar para completar la configuración inicial de Amazon SES, así como tutoriales que le ayudarán a comenzar a utilizar la herramienta.

Temas

- Configuración de Amazon Simple Email Service
- Migración a Amazon SES desde otra solución de envío de correo electrónico
- Solicitar acceso a la producción (salir del entorno de pruebas de Amazon SES)

Configuración de Amazon Simple Email Service

Para comenzar a utilizar Amazon SES, debe completar las tareas siguientes.

Tareas

- Inscríbase en AWS
- Configurar la cuenta de SES
- Adjudicar acceso mediante programación (para interactuar con SES fuera de la consola)
- Descargue un AWS SDK (para usar las API de SES)

Inscríbase en AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirse a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea una. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

Configurar la cuenta de SES

Comience con SES verificando una dirección de correo electrónico y un dominio de envío para que pueda empezar a enviar correos electrónicos a través de SES y solicitar el acceso de producción para la cuenta mediante el asistente de configuración de cuentas de SES.

Uso del asistente de configuración de cuentas de SES para configurar la cuenta

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. Seleccione Comenzar en la página de inicio de la consola de SES y el asistente le explicará los pasos necesarios para configurar la cuenta de SES.

El asistente de configuración de cuentas de SES solo aparecerá si aún no ha creado ninguna identidad (dirección de correo electrónico o dominio) en SES.

Adjudicar acceso mediante programación (para interactuar con SES fuera de la consola)

Los usuarios necesitan acceso programático si quieren interactuar con personas AWS ajenas a. AWS Management Console La forma de conceder el acceso programático depende del tipo de usuario que acceda. AWS

Para conceder acceso programático a los usuarios, elija una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	Mediante
Identidad del personal (Usuarios administrados en el IAM Identity Center)	Usa credenciales temporales para firmar las solicitudes programáticas a los AWS CLI AWS SDK o las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Configuración del uso AWS IAM Identity Center en AWS CLI la Guía del AWS Command Line Interface usuario.

¿Qué usuario necesita acceso programático?	Para	Mediante
		• Para obtener AWS información sobre los SDK, las herramientas y AWS las API, consulte la autenticación del IAM Identity Center en la Guía de referencia de AWS los SDK y las herramientas.
IAM	Utilice credenciales temporales para firmar las solicitudes programáticas a los AWS SDK o las AWS CLI API. AWS	Siga las instrucciones de Uso de credenciales temporales con AWS recursos de la Guía del usuario de IAM.

¿Qué usuario necesita acceso programático?	Para	Mediante
IAM	(No recomendado) Utilice credenciales de larga duración para firmar las solicitudes programáticas a los AWS CLI AWS SDK o las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Autenticación con credencia les de usuario de IAM en la Guía del usuario.AWS Command Line Interface • Para obtener informaci ón AWS sobre los SDK y las herramientas, consulte Autenticarse con credencia les de larga duración en la Guía de referencia de los AWS SDK y las herramien tas. • Para obtener informaci ón AWS sobre las API, consulte Administrar las claves de acceso para los usuarios de IAM en la Guía del usuario de IAM.

Descargue un AWS SDK (para usar las API de SES)

Para llamar a las API de SES sin tener que gestionar detalles de bajo nivel, como el ensamblaje de solicitudes HTTP sin procesar, puede usar un AWS SDK. Los AWS SDK proporcionan funciones y tipos de datos que encapsulan la funcionalidad de SES y otros servicios. AWS Para descargar un AWS SDK, vaya a los SDK. Tras descargar el SDK, cree un archivo de credenciales compartido y especifique las claves de AWS acceso.

Migración a Amazon SES desde otra solución de envío de correo electrónico

En este tema, se proporciona información general de los pasos que debe seguir si desea mover su solución de envío de correo electrónico a Amazon SES desde una solución alojada localmente o alojada en una instancia de Amazon EC2.

Temas de esta sección:

- Paso 1. Verificar su dominio
- Paso 2. Solicitar acceso de producción
- Paso 3. Configurar sistemas de autenticación de dominios
- Paso 4. Generar sus credenciales de SMTP
- Paso 5. Conectarse a un punto de enlace de SMTP
- Siguientes pasos

Paso 1. Verificar su dominio

Para poder usar Amazon SES para enviar mensajes de correo electrónico, debe verificar las identidades desde las que tiene previsto enviar correo electrónico. En Amazon SES, una identidad puede ser una dirección de correo electrónico o un dominio completo. Cuando verifique el dominio, podrá usar Amazon SES para enviar correo electrónico desde cualquier dirección de dicho dominio. Para obtener más información sobre la verificación de dominios, consulte Creación de una identidad de dominio.

Paso 2. Solicitar acceso de producción

La primera vez que utiliza Amazon SES, su cuenta se encuentra en un entorno de pruebas. Mientras la cuenta esté en el entorno de pruebas, solo podrá enviar correo electrónico a direcciones que haya verificado. Además, existen restricciones sobre el número de mensajes que puede enviar al día y el número que puede enviar por segundo. Para obtener más información sobre cómo solicitar acceso de producción, consulte Solicitar acceso a la producción (salir del entorno de pruebas de Amazon SES).

Paso 3. Configurar sistemas de autenticación de dominios

Puede configurar su dominio para que utilice sistemas de autenticación como DKIM y SPF. Este paso es opcional desde el punto de visto técnico. Sin embargo, al configurar DKIM o SPF (o ambos) para su dominio, puede mejorar la capacidad de entrega de sus mensajes de correo electrónico y aumentar la confianza que sus clientes tienen en usted. Para obtener más información sobre la configuración de SPF, consulte Autenticación de correo electrónico con SPF en Amazon SES. Para obtener más información acerca de la configuración de DKIM, consulte Autenticación de correo electrónico con DKIM en Amazon SES.

Paso 4. Generar sus credenciales de SMTP

Si tiene previsto enviar correo electrónico mediante una aplicación que utiliza SMTP, debe generar credenciales de SMTP. Sus credenciales de SMTP son distintas de las credenciales de AWS normales. Estas credenciales también son únicas en cada AWS región. Para obtener más información sobre cómo generar sus credenciales de SMTP, consulte Obtención de las credenciales de SMTP de Amazon SES.

Paso 5. Conectarse a un punto de enlace de SMTP

Si utiliza un agente de transferencia de mensajes como postfix o sendmail, debe actualizar la configuración de esa aplicación de forma que haga referencia a un punto de enlace SMTP de Amazon SES. Para obtener una lista completa de puntos de enlace SMTP, consulte Conexión a un punto de enlace de SMTP de Amazon SES. Tenga en cuenta que las credenciales SMTP que creó en el paso anterior están asociadas a una AWS región específica. Tiene que conectarse al punto de enlace SMTP en la región en la que creó las credenciales de SMTP.

Siguientes pasos

En este punto, ya está listo para comenzar a enviar correo electrónico utilizando Amazon SES. Sin embargo, hay algunos pasos opcionales que puede realizar.

- Puede crear conjuntos de configuración, que son conjuntos de reglas que se aplican a los mensajes de correo electrónico que envía. Por ejemplo, puede utilizar conjuntos de configuración para especificar dónde se envían las notificaciones cuando se entrega un correo electrónico, cuando un destinatario abre un mensaje o hace clic en un vínculo, cuando un correo electrónico produce un rebote y cuando un destinatario marca su correo electrónico como spam. Para obtener más información, consulte Uso de conjuntos de configuración en Amazon SES.

- Cuando envía correo electrónico a través de Amazon SES, es importante monitorear los rebotes y los reclamos de su cuenta. Amazon SES incluye una consola de métricas de reputación que puede utilizar para realizar un seguimiento de los rebotes y reclamos de su cuenta. Para obtener más información, consulte Uso de métricas de reputación para realizar un seguimiento de las tasas de rebotes y de reclamos. También puedes crear CloudWatch alarmas que te avisen cuando estas tarifas suban demasiado. Para obtener más información sobre la creación de CloudWatch alarmas, consulteCreación de alarmas de monitoreo de reputación en CloudWatch.
- Los clientes que envían un gran volumen de correo electrónico, o aquellos que simplemente desean tener un control total sobre la reputación de sus direcciones IP, pueden alquilar direcciones IP dedicadas pagando una cuota mensual adicional. Para obtener más información, consulte Direcciones IP dedicadas para Amazon SES.

Solicitar acceso a la producción (salir del entorno de pruebas de Amazon SES)

Para ayudarlo a evitar fraudes y abusos y a proteger su reputación como remitente, aplicamos determinadas restricciones a las cuentas nuevas de Amazon SES.

Colocamos todas las cuentas nuevas en el entorno de pruebas de Amazon SES. El estado de entorno limitado de su cuenta es único para cada una de ellas. Región de AWS Mientras su cuenta se encuentre en el entorno de pruebas, puede utilizar todas las características de Amazon SES. Sin embargo, cuando su cuenta está en el entorno de pruebas, aplicamos las siguientes restricciones a la misma:

- Solo puede enviar correo a direcciones correo electrónico y dominios verificados o al simulador de buzón de correo de Amazon SES.
- Puede enviar un máximo de 200 mensajes por cada periodo de 24 horas.
- Puede enviar un máximo de un mensaje por segundo.
- Para la autorización de envío, ni usted ni el remitente delegado pueden enviar correos electrónicos a direcciones de correo electrónico no verificadas.
- Para la supresión a nivel de la cuenta, las acciones masivas y las llamadas a la API de SES relacionadas con la administración de listas de supresión están desactivadas.

Cuando tu cuenta haya pasado del entorno limitado a la de producción, podrás enviar correos electrónicos a cualquier destinatario, independientemente de si la dirección o el dominio del

destinatario están verificados. Sin embargo, tiene que seguir verificando todas las identidades que utilice como direcciones "From", "Source", "Sender" o "Return-Path".

Complete los procedimientos de esta sección para solicitar que su cuenta se retire del entorno limitado y se ponga en producción.

> **Note**
>
> - Si aún no ha creado ninguna identidad (dirección de correo electrónico o dominio) en SES, puede omitir los procedimientos de esta página y solicitar el acceso de producción a su cuenta mediante el asistente de configuración de cuentas de SES. Consulte Configurar su cuenta SES para obtener instrucciones sobre cómo acceder al asistente.
> - Si utiliza Amazon SES para enviar correo electrónico desde una instancia de Amazon EC2, es posible que también tenga que solicitar que la limitación controlada se elimine del puerto 25 de la instancia de Amazon EC2. Para obtener más información, consulte ¿Cómo puedo quitar el acelerador del puerto 25 de mi instancia EC2? en el AWS Knowledge Center.

Para solicitar el acceso a la producción (eliminar tu cuenta del entorno de pruebas), utiliza el AWS Management Console

1. Abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, elija Panel de la cuenta.
3. En el cuadro de advertencia situado en la parte superior de la consola que dice “Your Amazon SES account is in the sandbox” (Su cuenta de Amazon SES está en el entorno de pruebas), en la parte derecha, elija Request production access (Solicitar acceso de producción).
4. En el modal de detalles de la cuenta, seleccione el botón de opción Marketing o Transactional (Transaccional) que mejor describa la mayoría del correo que va a enviar.

   - Correo electrónico de marketing: se envía one-to-many a una lista específica de prospectos o clientes y contiene contenido de marketing y promocional, por ejemplo, para realizar una compra, descargar información, etc.
   - Correo electrónico transaccional: se envía de one-to-one forma exclusiva a cada destinatario y normalmente se desencadena por una acción del usuario, como la compra de un sitio web, una solicitud de restablecimiento de contraseña, etc.

5. En Website URL (URL de sitio web), ingrese la URL de su sitio web para ayudarnos a comprender mejor el tipo de contenido que planea enviar.
6. En Use case description (Descripción de caso de uso), explique cómo tiene previsto utilizar Amazon SES para enviar correo electrónico. Para ayudarnos a procesar su solicitud, debe responder a las siguientes preguntas:
   - ¿Cómo tiene previsto crear o adquirir su lista de correo?
   - ¿Cómo tiene previsto gestionar los rebotes y las reclamaciones?
   - ¿Cómo pueden los destinatarios dejar de recibir correo electrónico de usted?
   - ¿Cómo eligió el ratio o la cuota de envío que ha especificado en esta solicitud?
7. En Additional contacts (Contactos adicionales), díganos dónde desea recibir comunicaciones acerca de su cuenta. Puede ser una lista separada por comas de hasta cuatro direcciones de correo electrónico.
8. En Preferred contact language (Idioma de contacto preferido), elija si desea recibir las comunicaciones en English (Inglés) o Japanese (Japonés).
9. En Acknowledgement (Confirmación), marque la casilla para aceptar enviar solo correo electrónico a personas que lo hayan solicitado explícitamente y confirme que tiene un proceso establecido para gestionar las notificaciones de rebotes y reclamos.
10. Elija el botón Submit request (Enviar solicitud): se mostrará un banner para confirmar que su solicitud se ha enviado y se encuentra actualmente en revisión.

Una vez que envíe una revisión de los detalles de su cuenta, no podrá editar los datos hasta que se haya completado la revisión. El AWS Support equipo proporciona una respuesta inicial a tu solicitud en un plazo de 24 horas.

Para evitar que nuestros sistemas sean utilizados para enviar contenido no solicitado o malicioso, tenemos que considerar cada solicitud detenidamente. Si podemos hacerlo, garantizaremos una solicitud en este periodo de 24 horas. Sin embargo, si tenemos que obtener información adicional suya, puede que la solicitud tarde más tiempo en concederse. Es posible que no podamos garantizar su solicitud si su caso de uso no está en consonancia con nuestras políticas.

Si lo desea, también puede enviar su solicitud de acceso a la producción utilizando el AWS CLI. Enviar su solicitud mediante el AWS CLI resulta útil cuando quiere solicitar acceso a la producción para un gran número de identidades o cuando quiere automatizar el proceso de configuración de Amazon SES.

Para solicitar que su cuenta se elimine del entorno de pruebas de Amazon SES mediante la AWS CLI

1. Requisito previo: tiene que instalar y configurar AWS CLI. Para obtener más información, consulte la Guía del usuario de AWS Command Line Interface.
2. En la línea de comandos, escriba el comando siguiente.

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

   En el comando anterior, haga lo siguiente.

   a. Reemplace *TRANSACTIONAL* por el tipo de correo electrónico que tiene previsto enviar a través de Amazon SES. Puede especificar `TRANSACTIONAL` o `PROMOTIONAL`. Si hay más de un valor aplicable, especifique la opción que se aplique a la mayoría de los correos electrónicos que vaya a enviar.
   b. Reemplace *https://example.com* por la dirección URL de su sitio web. Esta información nos ayuda a entender mejor el tipo de contenido que desea enviar.
   c. Reemplace *Use case description* (Descripción de caso de uso) por una descripción de cómo tiene previsto usar Amazon SES para enviar correo electrónico. Para ayudarnos a procesar su solicitud, debe responder a las siguientes preguntas:
      i. ¿Cómo tiene previsto crear o adquirir su lista de correo?
      ii. ¿Cómo tiene previsto gestionar los rebotes y las reclamaciones?
      iii. ¿Cómo pueden los destinatarios dejar de recibir correo electrónico de usted?
      iv. ¿Cómo eligió el ratio o la cuota de envío que ha especificado en esta solicitud?
   d. Reemplace *info@example.com* por las direcciones de email en las que desea recibir comunicaciones acerca de su cuenta. Puede ser una lista separada por comas de hasta cuatro direcciones de correo electrónico.
   e. Reemplace *EN* por el idioma que prefiera. Puede especificar `EN` para inglés o `JA` para japonés.

Una vez que envíe una revisión de los detalles de su cuenta, no podrá editar los datos hasta que se haya completado la revisión. El AWS Support equipo proporcionará una respuesta inicial a su solicitud en un plazo de 24 horas.

Para evitar que nuestros sistemas sean utilizados para enviar contenido no solicitado o malicioso, tenemos que considerar cada solicitud detenidamente. Si podemos hacerlo, garantizaremos una solicitud en este periodo de 24 horas. Sin embargo, si tenemos que obtener información adicional suya, puede que la solicitud tarde más tiempo en concederse. Es posible que no podamos garantizar su solicitud si su caso de uso no está en consonancia con nuestras políticas.

Administración de sus límites de envío de Amazon SES

Su cuenta de Amazon SES tiene un conjunto de cuotas de envío para regular el número de mensajes de correo electrónico que puede enviar y la velocidad a la que puede enviarlos. Las cuotas de envío benefician a todos los clientes de Amazon SES porque ayudan a mantener la relación de confianza entre Amazon SES y los proveedores de correo electrónico. Las cuotas de envío le ayudan a aumentar gradualmente su actividad de envío y a reducir la probabilidad de que los proveedores de correo electrónico bloqueen sus correos electrónicos, debido a picos inesperados en su frecuencia o volumen de envío de correo electrónico.

Las siguientes cuotas se aplican al envío de correo electrónico a través de Amazon SES:

- Cuota de envío: número máximo de correos electrónicos que puede enviar en un período de 24 horas. Esta cuota se calcula en un período de tiempo acumulativo. Cada vez que intenta enviar un correo electrónico, Amazon SES determina el número de correos electrónicos que envió en las últimas 24 horas. Siempre que el número total de correos electrónicos que ha enviado en las últimas 24 horas sea inferior a este máximo diario, su solicitud de envío será aceptada y su correo electrónico será enviado.

  Si el envío de un mensaje supera el máximo diario de su cuenta, se rechaza su llamada a Amazon SES.
- Tasa de envío: número máximo de mensajes de correo electrónico procedentes de su cuenta que Amazon SES puede aceptar por segundo. Puede superar esta cuota durante periodos cortos, pero no durante un periodo de tiempo prolongado.

  > **Note**
  >
  > La velocidad a la que Amazon SES acepta sus mensajes puede ser inferior a la velocidad máxima de envío de su cuenta.

- Tamaño máximo de mensaje (MB): tamaño máximo de un correo electrónico que puede enviar. Esto incluye las imágenes y los archivos adjuntos que forman parte del correo electrónico después de la codificación MIME. Por ejemplo, si adjunta un archivo de 5 MB, el tamaño del archivo adjunto en el correo electrónico después de la codificación MIME será de ~6,85 MB (aproximadamente el 137 % del tamaño del archivo original).

> **Note**
>
> Le recomendamos que cargue sus archivos adjuntos en las unidades de nube e incluya la URL de dichos archivos para reducir el tamaño del correo electrónico y mejorar la capacidad de entrega. SES no puede garantizar que los correos electrónicos de gran tamaño terminen en el buzón de correo del destinatario, ya que los diferentes servidores de correo tendrán políticas basadas en el tamaño variable.

Sus cuotas de envío de Amazon SES son independientes para cada región de AWS. Para obtener más información acerca del uso de Amazon SES en varias regiones de AWS, consulte Regiones y Amazon SES.

Cuando su cuenta está en el entorno de pruebas de Amazon SES, solo puede enviar 200 mensajes cada periodo de 24 horas y la velocidad máxima de envío es de un mensaje por segundo. Cuando envíe una solicitud para que su cuenta se elimine del entorno de pruebas, también puede solicitar que sus cuotas se incrementen al mismo tiempo. Para obtener más información sobre cómo sacar su cuenta del entorno de pruebas, consulte Solicitar acceso a la producción (salir del entorno de pruebas de Amazon SES).

Cuando su cuenta se haya eliminado del entorno de pruebas, puede solicitar aumentos adicionales de la cuota en cualquier momento creando una nueva incidencia en el Centro de AWS Support. Para obtener más información, consulte Aumento de las cuotas de envío de Amazon SES .

> **Note**
>
> Las cuotas de envío se basan en los destinatarios en lugar de en los mensajes. Por ejemplo, un correo electrónico que tenga 10 destinatarios se contabiliza como 10 en su cuota. Sin embargo, no es recomendable que envíe un correo electrónico a varios destinatarios en una sola llamada a la operación de la API `SendEmail`, ya que si la llamada produce un error, se rechaza todo el correo electrónico. Le recomendamos que llame a `SendEmail` una vez por cada destinatario.

- Para aumentar las cuotas de envío, consulte Aumento de las cuotas de envío de Amazon SES.
- Para monitorear sus cuotas de envío mediante la consola de Amazon SES o la API de Amazon SES, consulte Monitoreo de las cuotas de envío de Amazon SES.

- Para obtener información sobre los errores que recibe su aplicación al alcanzar las cuotas de envío, consulte Errores relacionados con las cuotas de envío de su cuenta de Amazon SES.

Aumento de las cuotas de envío de Amazon SES

Su cuenta tiene las siguientes cuotas por cada región actual y se puede aumentar.

Recurso	Cuota predeterminada	Descripción
Cuota de envío	200	El número máximo de correos electrónicos que puede enviar en un periodo de 24 horas para esta cuenta en la Región de AWS actual.
Tasa de envío	1	Número máximo de mensajes de correo electrónico que Amazon SES puede aceptar cada segundo para esta cuenta en la Región de AWS actual.

Aumento automático de las cuotas de envío

Cuando su cuenta está fuera del entorno de pruebas y va a enviar correo electrónico de producción de alta calidad, podríamos aumentar automáticamente las cuotas de envío de su cuenta. A menudo, aumentamos automáticamente estas cuotas antes de que necesite aumentarlas.

Para poder optar a aumentos de ratio automáticos, tienen que cumplirse todas las afirmaciones siguientes:

- Envía contenido de alta calidad que sus destinatarios desean recibir: envíe contenido que los destinatarios desean y esperan. Deje de enviar correo electrónico a los clientes que no lo abren.
- Envía contenido de producción real: enviar mensajes de prueba a direcciones de email ficticias puede afectar de manera negativa a sus tasas de rebotes y reclamos. Además, enviar mensajes únicamente a destinatarios internos hace que sea difícil determinar si envía contenido que los clientes desean recibir. Sin embargo, cuando envía los mensajes de producción a destinatarios que no son internos, podemos evaluar de forma precisa sus prácticas de envío de correo electrónico.

- Envía correo electrónico hasta casi alcanzar su cuota actual: para tener derecho a un aumento automático del límite, su volumen de correo electrónico diario debe aproximarse en su cuenta sin superarlo.
- Tiene tasas bajas de rebotes y reclamos: reduzca al mínimo el número de rebotes y reclamos que recibe. Tener un número elevado de rebotes y reclamaciones puede afectar negativamente a sus cuotas de envío.

El usuario solicitó un aumento de las cuotas de envío

Si las cuotas de envío actuales no son suficientes para sus necesidades y no las hemos aumentado automáticamente, puede solicitar un aumento:

- Cuota de envío o tasa de envío: las solicitudes de aumento de cualquiera de estas se pueden enviar a través de la Consola de AWS Service Quotas.

Para solicitar un aumento de las cuotas de envío de Amazon SES mediante la consola de Service Quotas

1. Abra la consola de Service Quotas.
2. Seleccione la región para la que desea el aumento mediante el menú desplegable situado en la esquina superior derecha de la consola (junto al número de cuenta).
3. En el panel de navegación, elija AWS services (Servicios de AWS).
4. Elija Amazon Simple Email Service (SES).
5. Elija una cuota y siga las instrucciones para solicitar un aumento de cuota.

SLA del equipo de AWS Support para aumentar los tipos de solicitudes

Para evitar que nuestros sistemas sean utilizados para enviar contenido no solicitado o malicioso, tenemos que considerar cada solicitud detenidamente. Si podemos hacerlo, confirmaremos su solicitud en los tiempos especificados que se indican a continuación para el tipo de aumento solicitado. Sin embargo, si tenemos que obtener información adicional suya, puede que la solicitud tarde más tiempo en concederse. Es posible que no podamos confirmar su solicitud si su caso de uso no está en consonancia con nuestras políticas.

- Cuota de envío o tasa de envío: hasta 24 horas.

> **Note**
>
> Aunque la consola de Service Quotas está disponible en muchos idiomas diferentes, el soporte real solo se proporciona en inglés.

Monitoreo de las cuotas de envío de Amazon SES

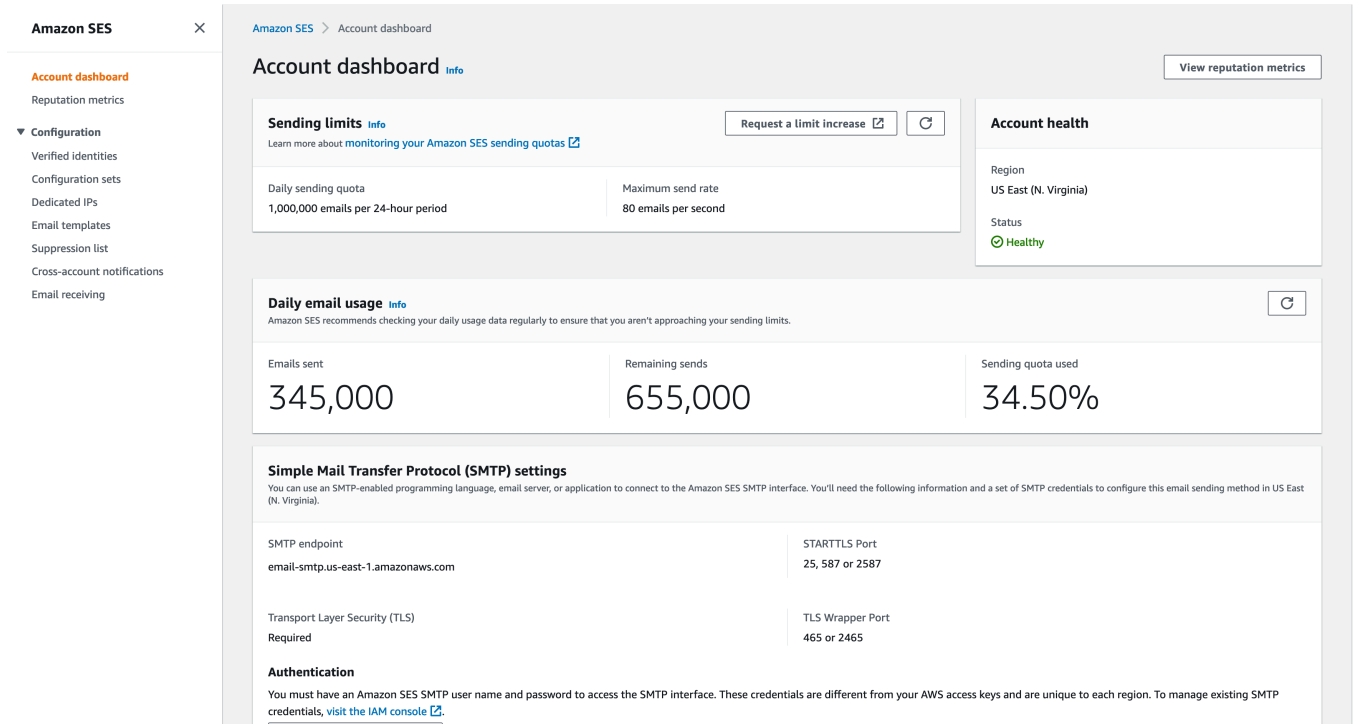
Puede monitorear sus cuotas de envío mediante la consola de Amazon SES o a través de la API de Amazon SES, ya sea directamente mediante una llamada a la interfaz de consultas (HTTPS) o indirectamente a través de un SDK de AWS, la AWS Command Line Interface o las AWS Tools for Windows PowerShell.

> **Important**
>
> Le recomendamos que consulte con frecuencia sus estadísticas de envío, a fin de asegurarse de que no está cerca de sus cuotas de envío. Si está cerca de sus cuotas de envío, consulte Aumento de las cuotas de envío de Amazon SES para obtener información acerca de cómo aumentarlas. No espere a alcanzar las cuotas de envío para plantearse aumentarlas.

Monitoreo de las cuotas de envío mediante la consola de Amazon SES

El siguiente procedimiento muestra cómo ver sus cuotas de envío mediante la consola de Amazon SES.

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, elija Account dashboard (Panel de la cuenta). Sus cuotas de envío se muestran en Sending Limits (Límites de envío). El total de correos electrónicos enviados, los envíos restantes y el porcentaje de la cuota de envío utilizada se muestran en Daily email usage (Uso diario del correo electrónico).



3. Para actualizar la pantalla, haga clic en el icono de actualización que aparece en la esquina superior derecha del cuadro Daily email usage (Uso diario del correo electrónico).

Monitoreo de las cuotas de envío mediante la API de Amazon SES

La API de Amazon SES ofrece la acción `GetSendQuota`, que devuelve las cuotas de envío actuales. Cuando llame a la acción `GetSendQuota`, recibe la información siguiente:

- Número de mensajes de correo electrónico que ha enviado durante las últimas 24 horas
- Cuota de envío para el periodo de 24 horas actual
- Tasa de envío máxima

> **Note**
>
> Para obtener una descripción de `GetSendQuota`, consulte la Referencia de la API de Amazon Simple Email Service.

Errores relacionados con las cuotas de envío de su cuenta de Amazon SES

Si intenta enviar un correo electrónico después de alcanzar su cuota de envío diaria (la cantidad máxima de correo electrónico que puede enviar en un periodo de 24 horas) o su velocidad máxima de envío (el número máximo de mensajes que puede enviar por segundo), Amazon SES elimina el mensaje y no intenta enviarlo de nuevo. Amazon SES también proporciona un mensaje de error que explica el problema. La forma en que Amazon SES produce este mensaje de error depende de cómo intentó enviar el correo electrónico. En este tema, se incluye información acerca de los mensajes que recibe a través de la API de Amazon SES y a través de la interfaz de SMTP.

Para conocer la técnica que puede utilizar cuando se alcanza la velocidad máxima de envío, consulte How to handle a "Throttling – Maximum sending rate exceeded" error en el Blog de mensajería y segmentación de AWS.

Alcanzar límites de envío con la API de Amazon SES

Si intenta enviar un email a través de la API de Amazon SES (o un SDK de AWS), pero ya ha superado los límites de envío de su cuenta, la API produce un error `ThrottlingException`. El mensaje de error incluye uno de los siguientes mensajes:

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

Si encuentra un error de limitación controlada, debe programar su aplicación para que espere un intervalo de hasta 10 minutos y, a continuación, vuelva a intentar la solicitud de envío.

Alcanzar límites de envío con SMTP

Si intenta enviar un correo electrónico utilizando la interfaz de SMTP de Amazon SES, pero ya ha superado los límites de envío de su cuenta, es posible que su cliente SMTP muestre uno de los siguientes errores:

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

Los diferentes clientes de SMTP controlan estos errores de distintas formas.

Configurar el envío de correo electrónico con Amazon SES

Puede enviar un email con Amazon Simple Email Service (Amazon SES) mediante la consola de Amazon SES, la interfaz Simple Mail Transfer Protocol (SMTP) de Amazon SES o la API de Amazon SES. Normalmente, la consola se utiliza para enviar correos electrónicos de prueba y para administrar su actividad de envío. Para enviar correos electrónicos masivos, se utiliza la interfaz de SMTP o la API. Para obtener información acerca de los precios de email de Amazon SES, consulte Precios de Amazon SES.

- Si desea utilizar un paquete de software, una aplicación o un lenguaje de programación habilitado para SMTP a fin de enviar email a través de Amazon SES o integrar Amazon SES con su servidor de email actual, utilice la interfaz de SMTP de Amazon SES. Para obtener más información, consulte Envío de correo electrónico mediante programación con la interfaz de SMTP de Amazon SES.
- Si desea llamar a Amazon SES mediante solicitudes HTTP sin procesar, utilice la API de Amazon SES. Para obtener más información, consulte Uso de la API de Amazon SES para enviar correo electrónico.

> **Important**
>
> Cuando envíe un email a varios destinatarios (los destinatarios “To”, “CC” y “BCC”) y la llamada a Amazon SES devuelva un error, se rechaza todo el email y ninguno de los destinatarios recibirá el email. Por lo tanto, recomendamos que envíe un correo electrónico a un destinatario cada vez.

Uso de la interfaz de SMTP de Amazon SES para enviar correo electrónico

Para enviar email de producción a través de Amazon SES, puede utilizar la interfaz de Simple Mail Transfer Protocol (SMTP) o la API de Amazon SES. Para obtener más información acerca de la API de Amazon SES, consulte Uso de la API de Amazon SES para enviar correo electrónico. En esta sección, se describe la interfaz de SMTP.

Amazon SES envía correo electrónico a través de SMTP, que es el protocolo de correo electrónico más común en Internet. Puede enviar correo electrónico a través de Amazon SES con una amplia

variedad de software y lenguajes de programación habilitados para SMTP para conectarse a la interfaz de SMTP de Amazon SES. En esta sección, se explica cómo obtener las credenciales de SMTP de Amazon SES, cómo enviar email a través de la interfaz de SMTP y cómo configurar varios servidores de correo electrónico y programas de software para utilizar Amazon SES con el fin de enviar correo electrónico.

Para obtener soluciones a problemas comunes que podría encontrar al utilizar Amazon SES a través de la interfaz SMTP, consulte Problemas de SMTP de Amazon SES.

Requisitos para enviar correo electrónico a través de SMTP

Para enviar correo electrónico a través de la interfaz de SMTP de Amazon SES, necesita lo siguiente:

- La dirección del punto de enlace SMTP. Para obtener una lista de puntos de enlace de SMTP de Amazon SES, consulte Conexión a un punto de enlace de SMTP de Amazon SES.
- El número de puerto de la interfaz de SMTP. El número de puerto varía según el método de conexión. Para obtener más información, consulte Conexión a un punto de enlace de SMTP de Amazon SES.
- Un nombre de usuario y contraseña de SMTP. Las credenciales de SMTP son exclusivas para cada región de AWS . Si tiene previsto utilizar la interfaz de SMTP para enviar correo electrónico en varias regiones de AWS , necesita credenciales de SMTP para cada región.

> **Important**
>
> Sus credenciales SMTP no son idénticas a sus claves de AWS acceso ni a las credenciales que utiliza para iniciar sesión en la consola Amazon SES. Para obtener información acerca de cómo generar sus credenciales de SMTP, consulte Obtención de las credenciales de SMTP de Amazon SES.

- Software cliente que permite las comunicaciones mediante Transport Layer Security (TLS). Para obtener más información, consulte Conexión a un punto de enlace de SMTP de Amazon SES.
- Una dirección de correo electrónico verificada con Amazon SES. Para obtener más información, consulte Identidades verificadas en Amazon SES.
- Mayores cuotas de envío, si desea enviar grandes cantidades de correo electrónico. Para obtener más información, consulte Administración de sus límites de envío de Amazon SES.

Métodos para enviar correo electrónico a través de SMTP

Puede enviar correo electrónico a través de SMTP mediante cualquiera de los métodos siguientes:

- Si desea configurar cualquier software habilitado para SMTP con el fin de enviar correo electrónico a través de la interfaz de SMTP de Amazon SES, consulte Envío de correo electrónico a través de Amazon SES mediante paquetes de software.
- Para programar una aplicación para enviar correo electrónico a través de Amazon SES, consulte Envío de correo electrónico mediante programación con la interfaz de SMTP de Amazon SES.
- Para configurar su servidor de correo electrónico existente para enviar todo el correo saliente a través de Amazon SES, consulte Integración de Amazon SES con su servidor de correo electrónico existente.
- Para interactuar con la interfaz de SMTP de Amazon SES mediante la línea de comandos, lo que puede resultar útil para hacer pruebas, consulte Prueba de la conexión a la interfaz SMTP de Amazon SES mediante la línea de comandos.

Para ver una lista de códigos de respuesta de SMTP, consulte Códigos de respuesta de SMTP devueltos por Amazon SES..

Información de correo electrónico que se debe facilitar

Cuando acceda a Amazon SES a través de la interfaz de SMTP, la aplicación cliente de SMTP creará el mensaje, por lo que la información que es necesario proporcionar depende de la aplicación que se utilice. Como mínimo, el intercambio SMTP entre un cliente y un servidor requiere los elementos siguientes:

- Dirección de origen
- Dirección de destino
- Datos del mensaje

Si utiliza la interfaz de SMTP y tiene habilitado el reenvío de retroalimentación, las notificaciones de rebotes, reclamaciones y entrega se envían a la dirección "MAIL FROM". No se utiliza ninguna dirección "Reply-To" que especifique.

Obtención de las credenciales de SMTP de Amazon SES

Necesita las credenciales de SMTP de Amazon SES para acceder a la interfaz de SMTP de SES.

Las credenciales que utiliza para enviar correos electrónicos a través de la interfaz SMTP de SES son exclusivas de cada AWS región. Si utiliza la interfaz de SMTP de SES para enviar correo electrónico en más de una región, deberá generar un conjunto de credenciales de SMTP para cada región que tenga previsto usar.

Su contraseña SMTP es diferente de su clave de acceso AWS secreta. Para obtener más información acerca de las credenciales, consulte Tipos de credenciales de Amazon SES.

> **Note**
>
> Los puntos de conexión SMTP no están disponibles actualmente en África (Ciudad del Cabo), Asia Pacífico (Yakarta), Europa (Milán), Israel (Tel Aviv) y Oriente Medio (Bahréin).

Obtención de credenciales de SMTP de SES con la consola de SES

Al usar el flujo de trabajo de SES siguiente para generar credenciales SMTP a través de la consola, se le redirige a la consola de IAM para crear un usuario con las políticas adecuadas para llamar a SES y se le proporcionan las credenciales de SMTP asociadas a dicho usuario.

Requisito

Un usuario de IAM puede crear credenciales de SMTP de SES, pero la política de usuario puede concederle permiso para utilizar el propio IAM, dado que las credenciales de SMTP de SES se crean mediante IAM. La política de IAM debe permitirle realizar las siguientes acciones de IAM: `iam:ListUsers`, `iam:CreateUser`, `iam:CreateAccessKey` e `iam:PutUserPolicy`. Si intenta crear las credenciales SMTP de SES mediante la consola y su usuario de IAM no tiene estos permisos, aparecerá un error que indica que su cuenta «no está autorizada para realizar iam:». ListUsers

Para crear sus credenciales de SMTP

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.

2. Elija SMTP settings (Configuración de SMTP) en el panel de navegación de la izquierda. Se abrirá la página Simple Mail Transfer Protocol (SMTP) settings (Configuración del protocolo simple de transferencia de correo [SMTP]).
3. Elija Create SMTP Credentials (Crear credenciales SMTP) en la esquina superior derecha. Se abrirá la consola de IAM.
4. (Opcional) Si necesita ver, editar o eliminar los usuarios de SMTP que ya ha creado, elija Manage my existing SMTP credentials (Administrar mis credenciales de SMTP existentes) en la esquina inferior derecha. Se abrirá la consola de IAM. Los detalles para administrar las credenciales de SMTP se proporcionan siguiendo estos procedimientos.
5. En Crear usuario para SMTP, escriba un nombre para el usuario de SMTP en el campo Nombre de usuario. También puede utilizar el valor predeterminado que se proporciona en este campo. Cuando haya terminado, elija Crear usuario en la esquina inferior derecha.
6. Seleccione Mostrar en la Contraseña SMTP: las credenciales de SMTP se muestran en la pantalla.
7. Elija Descargar archivo .csv para descargar estas credenciales o cópielas y almacénelas en un lugar seguro, ya que no podrá ver ni guardar las credenciales después de haber cerrado este cuadro de diálogo.
8. Elija Volver a la consola de SES.

Puede ver una lista de las credenciales de SMTP que ha creado mediante este procedimiento en la consola de IAM en Access management (Administración de accesos) y elegir Users (Usuarios) seguido de la barra de búsqueda para encontrar a todos los usuarios a los que ha asignado credenciales de SMTP.

También puede utilizar la consola de IAM para eliminar usuarios de SMTP existentes. Para obtener más información sobre cómo eliminar usuarios, consulte Administración de usuarios de IAM en la Guía de introducción de IAM.

Si desea cambiar la contraseña de SMTP, elimine el usuario de SMTP existente en la consola de IAM. A continuación, para generar un nuevo conjunto de credenciales de SMTP, realice los procedimientos anteriores.

Obtener las credenciales SMTP de SES mediante la conversión de las credenciales existentes AWS

Si tiene un usuario que ha configurado mediante la interfaz de IAM, puede derivar las credenciales SMTP de SES del usuario a partir de sus credenciales. AWS

> **Important**
>
> No utilice AWS credenciales temporales para obtener las credenciales SMTP. La interfaz de SMTP de SES no es compatible con las credenciales de SMTP que se han generado a partir de credenciales de seguridad temporales.

Para habilitar el usuario de IAM con el fin de enviar correo electrónico a través de la interfaz de SMTP de SES, haga lo siguiente.

- Obtenga las credenciales SMTP del usuario a partir de sus AWS credenciales mediante el algoritmo que se proporciona en esta sección. Como se parte de las AWS credenciales, el nombre de usuario de SMTP es el mismo que el ID de la clave de AWS acceso, por lo que solo necesita generar la contraseña de SMTP.
- Aplique la siguiente política al usuario de IAM:

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

Para obtener más información sobre el uso de SES con IAM, consulte Identity and Access Management en Amazon SES.

> **Note**
>
> Aunque puede generar credenciales de SMTP de SES para cualquier usuario de IAM, le recomendamos que cree un usuario de IAM independiente cuando genere las credenciales de SMTP. Para obtener información acerca de por qué es una práctica recomendable crear usuarios para fines específicos, acceda a Prácticas recomendadas de IAM.

El siguiente pseudocódigo muestra el algoritmo que convierte una clave de acceso AWS secreta en una contraseña SMTP de SES.

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

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

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

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

Algunos lenguajes de programación incluyen bibliotecas que puede utilizar para convertir una clave de acceso secreta de IAM en una contraseña de SMTP. Esta sección incluye un ejemplo de código que puede utilizar para convertir una clave de acceso AWS secreta en una contraseña SMTP de SES mediante Python.

> **Note**
>
> En el siguiente ejemplo, se utilizan f-strings que se introdujeron en Python 3.6; si usa una versión anterior, no funcionarán.

Actualmente, el SDK de Python (Boto3) es oficialmente compatible con las versiones 2.7 y 3.6 (o posteriores). Sin embargo, la compatibilidad con la versión 2.7 es obsoleta y se descartará el 15/7/2021, por lo que deberá actualizarse al menos a la 3.6.

Python

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

import hmac
import hashlib
import base64
import argparse

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

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


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

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

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


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


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

Para obtener la contraseña de SMTP mediante este script, guarde el código anterior como `smtp_credentials_generate.py`. A continuación, en la línea de comandos, ejecute el comando siguiente:

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

En el comando anterior, haga lo siguiente.

- Reemplace *path/to/* con la ruta de acceso a la ubicación donde guardó `smtp_credentials_generate.py`.
- Sustituya *wJALRXUTNFEMI/K7MDEng/B PxRfi CYEXAMPLEKEY por la clave de acceso* secreta que desee convertir en una contraseña SMTP.
- Sustituya *us-east-1* por AWS la región en la que desee utilizar las credenciales SMTP.

Cuando este script se ejecuta correctamente, el único resultado es la contraseña de SMTP.

Conexión a un punto de enlace de SMTP de Amazon SES

Para enviar email mediante la interfaz de SMTP de Amazon SES, tiene que conectar su aplicación a un punto de enlace de SMTP. Para obtener una lista completa de los puntos de conexión de SMTP de Amazon SES, consulte Puntos de conexión y cuotas de Amazon Simple Email Service en la Referencia general de AWS.

El punto de enlace de SMTP de Amazon SES requiere que todas las conexiones se cifren con Transport Layer Security (TLS). (Tenga en cuenta que TLS se denomina en ocasiones con el nombre de su protocolo predecesor, SSL). Amazon SES admite dos mecanismos para establecer la conexión cifrada por TLS: STARTTLS y TLS Wrapper. Consulte la documentación de su software para determinar si es compatible con STARTTLS, TLS Wrapper o ambos.

De forma predeterminada, Amazon Elastic Compute Cloud (Amazon EC2) limita de manera controlada el tráfico de correo electrónico en el puerto 25. Para evitar tiempos de espera al enviar correo electrónico a través del punto de enlace de SMTP desde EC2, envíe una Solicitud de eliminación de limitaciones de envío de correo electrónico para eliminar la limitación. También puede enviar correo electrónico mediante otro puerto o utilizar un punto de enlace de Amazon VPC.

En caso de problemas con la conexión SMTP, consulte Problemas de SMTP.

STARTTLS

STARTTLS es un medio para actualizar una conexión sin cifrar a una conexión cifrada. Existen versiones de STARTTLS para diversos protocolos; la versión de SMTP se define en RFC 3207.

Para configurar una conexión STARTTLS, el cliente de SMTP se conecta con el punto de enlace de SMTP de Amazon SES en el puerto 25, 587 o 2587, emite un comando EHLO y espera a que el servidor anuncie que es compatible con la extensión de SMTP STARTTLS. A continuación, el cliente

emite el comando STARTTLS, iniciando la negociación de TLS. Cuando se completa la negociación, el cliente emite un comando EHLO sobre la nueva conexión cifrada y la sesión de SMTP continúa con normalidad.

TLS Wrapper

TLS Wrapper (también conocido como SMTPS o protocolo Handshake) es un medio de iniciar una conexión cifrada sin establecer primero una conexión sin cifrar. Con TLS Wrapper, el punto de enlace de SMTP de Amazon SES no realiza la negociación de TLS: es responsabilidad del cliente conectarse al punto de enlace mediante TLS y seguir utilizando TLS para toda la conversación. TLS Wrapper es un protocolo más antiguo, pero muchos clientes siguen siendo compatibles.

Para configurar una conexión de TLS Wrapper, el cliente de SMTP se conecta al punto de enlace de SMTP de Amazon SES en el puerto 465 o 2465. El servidor presenta su certificado, el cliente emite un comando EHLO y la sesión de SMTP continúa con normalidad.

Envío de correo electrónico a través de Amazon SES mediante paquetes de software

Existe una serie de paquetes de software comerciales y de código abierto que admiten el envío de correo electrónico a través de SMTP. Estos son algunos ejemplos:

- Plataformas de blog
- Agregadores RSS
- Software de administración de listas
- Sistemas de flujo de trabajo

Puede configurar cualquier software habilitado para SMTP de este tipo para enviar correo electrónico a través de la interfaz de SMTP de Amazon SES. Para obtener instrucciones sobre cómo configurar SMTP para un determinado paquete de software, consulte la documentación de dicho software.

El siguiente procedimiento muestra cómo configurar el envío de Amazon SES en JIRA, una conocida solución de seguimiento de problemas. Con esta configuración, JIRA puede notificar a los usuarios por correo electrónico cuando haya un cambio en el estado de un problema de software.

Para configurar JIRA con el fin de enviar correo electrónico mediante Amazon SES

1. Con su navegador web, inicie sesión en JIRA con credenciales de administrador.

2. En la ventana del navegador, elija Administration.
3. En el menú System, elija Mail.
4. En la página Mail administration, elija Mail Servers.
5. Elija Configure new SMTP mail server.
6. En el formulario Add SMTP Mail Server, rellene los campos siguientes:

   a. Name: un nombre descriptivo para este servidor.

   b. From address (Dirección desde): la dirección desde la que se enviará el correo electrónico. Antes de enviar correo electrónico a través de Amazon SES, tendrá que verificar esta dirección. Para obtener más información sobre la verificación, consulte Identidades verificadas en Amazon SES.

   c. Email prefix: una cadena que JIRA añade a cada línea de asunto antes del envío.

   d. Protocol: elija SMTP.

   > **Note**
   >
   > Si no puede conectarse a Amazon SES mediante esta configuración, pruebe SECURE_SMTP.

   e. Host Name (Nombre de host): consulte Conexión a un punto de enlace de SMTP de Amazon SES para ver un listado de puntos de enlace de SMTP de Amazon SES. Por ejemplo, si desea utilizar el punto de enlace de Amazon SES en la región EE. UU. Oeste (Oregón), el nombre del host sería email-smtp.us-west-2.amazonaws.com.

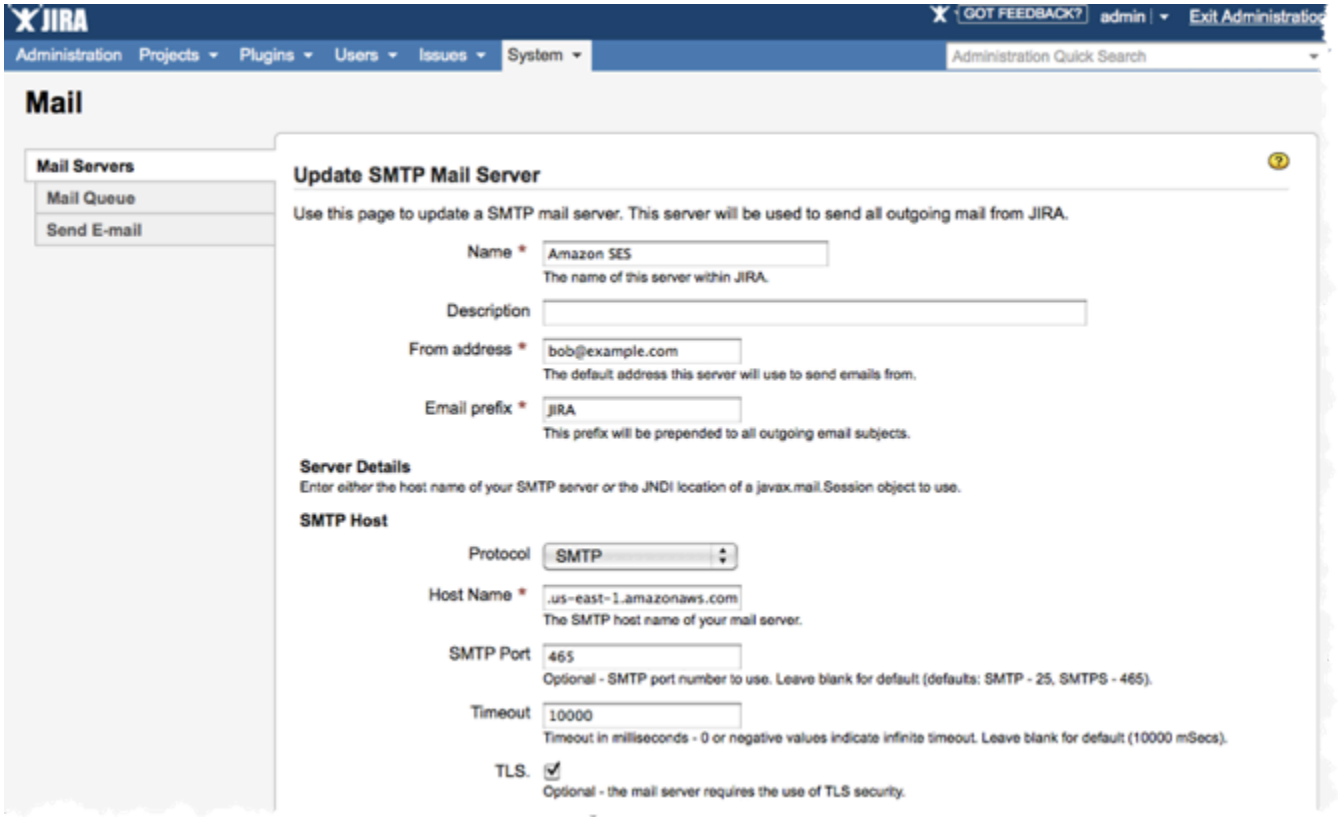
   f. SMTP Port (Puerto SMTP): 25, 587 o 2587 (para conectarse utilizando STARTTLS) o 465 o 2465 (para conectarse utilizando TLS Wrapper).

   g. TLS: seleccione esta casilla de verificación.

   h. User Name (Nombre de usuario): su nombre de usuario de SMTP.

   i. Password: su contraseña de SMTP.

   En la imagen siguiente se muestra la configuración de TLS Wrapper.



7. Elija Test Connection. Si el correo electrónico de prueba que envía JIRA a través de Amazon SES llega correctamente, su configuración está completa.

Envío de correo electrónico mediante programación con la interfaz de SMTP de Amazon SES

Para enviar un correo electrónico a través de la interfaz de SMTP de Amazon SES, puede utilizar un lenguaje de programación, servidor de email o aplicación habilitados para SMTP. Antes de comenzar, complete las tareas de Configuración de Amazon Simple Email Service. También tiene que obtener la siguiente información:

- Sus credenciales de SMTP de Amazon SES, que le permitirán conectarse al punto de conexión de SMTP de Amazon SES. Para obtener las credenciales de SMTP de Amazon SES, consulte Obtención de las credenciales de SMTP de Amazon SES.

> **Important**
>
> Sus credenciales SMTP son diferentes de las suyas. AWS Para obtener más información acerca de las credenciales, consulte Tipos de credenciales de Amazon SES.

- La dirección del punto de enlace SMTP. Para obtener una lista de puntos de enlace de SMTP de Amazon SES, consulte Conexión a un punto de enlace de SMTP de Amazon SES.
- El número de puerto de la interfaz de SMTP de Amazon SES, que depende del método de conexión. Para obtener más información, consulte Conexión a un punto de enlace de SMTP de Amazon SES.

Integración de Amazon SES con su servidor de correo electrónico existente

Si actualmente administra su propio servidor de correo electrónico, puede utilizar el punto de enlace de SMTP de Amazon SES para enviar todo su correo electrónico saliente a Amazon SES. No es necesario modificar sus clientes de correo electrónico y las aplicaciones existentes; la transición a Amazon SES pasará desapercibida para ellos.

Diversos agentes de transferencia de correo (MTA) admiten el envío de correo electrónico a través de relés de SMTP. En esta sección, se proporciona información general acerca de cómo configurar algunos MTA conocidos para enviar correo electrónico a través de la interfaz de SMTP de Amazon SES.

El punto de enlace de SMTP de Amazon SES requiere que todas las conexiones se cifren con Transport Layer Security (TLS).

Temas

- Integración de Amazon SES con SMTP de IIS de Microsoft Windows Server

Integración de Amazon SES con SMTP de IIS de Microsoft Windows Server

Puede configurar el servidor SMTP de IIS de Microsoft Windows Server para enviar correo electrónico a través de Amazon SES. Estas instrucciones se han escrito según el uso de Microsoft Windows Server 2012 en una instancia de Amazon EC2. Puede utilizar la misma configuración en Microsoft Windows Server 2008 y Microsoft Windows Server 2008 R2.

> **Note**
>
> Windows Server es una aplicación de terceros y no está desarrollada ni respaldada por Amazon Web Services. Los procedimientos de esta sección se proporcionan únicamente con fines informativos y están sujetos a cambios sin previo aviso.

Para integrar el servidor SMTP de IIS de Microsoft Windows Server con Amazon SES

1. En primer lugar, configure Microsoft Windows Server 2012 con las siguientes instrucciones.
   a. En la consola de administración de Amazon EC2, lance una nueva instancia base de Amazon EC2 para Microsoft Windows Server 2012.
   b. Conéctese a la instancia e inicie sesión en ella mediante el Escritorio remoto, según las instrucciones de Introducción a las instancias de Amazon EC2 para Windows.
   c. Lanzar el panel de Server Manager.
   d. Instale el rol Web Server. Asegúrese de incluir las herramientas de Compatibilidad con la administración de IIS 6 (una opción en la casilla de verificación Web Server).
   e. Instale la característica SMTP Server.
2. A continuación, configurar el servicio de SMTP IIS con las siguientes instrucciones.
   a. Vuelva al panel de Server Manager.
   b. En el menú Tools, elija Internet Information Services (IIS) 6.0 Manager.
   c. Haga clic con el botón derecho en SMTP Virtual Server #1 y, a continuación, seleccione Properties.
   d. En la pestaña Access, en Relay Restrictions, elija Relay.
   e. En el cuadro de diálogo Relay Restrictions, elija Add.
   f. En Single Computer, introduzca 127.0.0.1 para la dirección IP. Ahora ha concedido acceso para que este servidor retransmita email a Amazon SES a través del servicio SMTP de IIS.

      En este procedimiento, suponemos que sus correos electrónicos se generan en este servidor. Si la aplicación que genera el correo electrónico se ejecuta en un servidor independiente, debe conceder acceso de retransmisión para dicho servidor en SMTP de IIS.

> **Note**
>
> Para ampliar el relé de SMTP a subredes privadas, para Relay Restriction, utilice Single Computer 127.0.0.1 y Group of Computers 172.1.1.0 - 255.255.255.0 (en la sección de máscara de red). Para Connection, use Single Computer 127.0.0.1 y Group of Computers 172.1.1.0 - 255.255.255.0 (en la sección de máscara de red).

3. Por último, configure el servidor para enviar correo electrónico a través de Amazon SES con las siguientes instrucciones.

   a. Vuelva al cuadro de diálogo SMTP Virtual Server #1 Properties y, a continuación, elija la pestaña Delivery.

   b. En la pestaña Delivery, elija Outbound Security.

   c. Seleccione Basic Authentication (Autenticación básica) y, a continuación, ingrese sus credenciales de SMTP de Amazon SES. Puede obtener estas credenciales desde la consola de Amazon SES si sigue el procedimiento descrito en Obtención de las credenciales de SMTP de Amazon SES.

   > **Important**
   >
   > Sus credenciales SMTP no son las mismas que su identificador de clave de AWS acceso y su clave de acceso secreta. No intente utilizar sus AWS credenciales para autenticarse en el punto final SMTP. Para obtener más información acerca de las credenciales, consulte Tipos de credenciales de Amazon SES.

   d. Asegúrese de que TLS encryption está seleccionado.

   e. Vuelva a la pestaña Delivery.

   f. Elija Outbound Connections.

   g. En el cuadro de diálogo Outbound Connections, asegúrese de que el puerto sea 25 o 587.

   h. Seleccione Avanzado.

   i. Para el nombre del Smart host (Anfitrión inteligente), ingrese el punto de enlace de Amazon SES de que utilizará (por ejemplo, email-smtp.us-west-2.amazonaws.com). Para obtener una lista de las direcciones URL de los puntos de conexión Regiones de AWS en los que Amazon SES está disponible, consulte Amazon Simple Email Service (Amazon SES) en el. Referencia general de AWS

j. Vuelva al panel de Server Manager.

k. En el panel de Server Manager, haga clic con el botón derecho en SMTP Virtual Server # 1 y, a continuación, reinicie el servicio para recoger la nueva configuración.

l. Envíe un correo electrónico a través de este servidor. Puede examinar los encabezados de mensaje para confirmar que se ha entregado a través de Amazon SES.

Prueba de la conexión a la interfaz SMTP de Amazon SES mediante la línea de comandos

Puede utilizar los métodos descritos en esta sección desde la línea de comandos para probar la conexión con el punto de enlace SMTP de Amazon SES, validar las credenciales de SMTP y solucionar problemas de conexión. Estos procedimientos utilizan herramientas y bibliotecas que se incluyen con los sistemas operativos más comunes.

Para obtener información acerca de cómo solucionar problemas con las conexiones SMTP, consulte Problemas de SMTP de Amazon SES.

Requisitos previos

Cuando se conecta a la interfaz SMTP de Amazon SES, debe proporcionar un conjunto de credenciales de SMTP. Estas credenciales SMTP son diferentes de las credenciales estándar AWS . Los dos tipos de credenciales no son intercambiables. Para obtener más información sobre cómo obtener sus credenciales de SMTP, consulte the section called “Obtención de las credenciales de SMTP”.

Prueba de la conexión a la interfaz de SMTP de Amazon SES

Puede utilizar la línea de comandos para probar su conexión a la interfaz de SMTP de Amazon SES sin autenticar ni enviar ningún mensaje. Este procedimiento es útil para solucionar problemas de conectividad básicos. Si la conexión de prueba produce un error, consulte Problemas de SMTP.

En esta sección se incluyen procedimientos para probar la conexión mediante OpenSSL (que se incluye en la mayoría de las distribuciones de Linux, macOS y Unix, y también está disponible para Windows) como `Test-NetConnection` el cmdlet PowerShell in (que se incluye en las versiones más recientes de Windows).

Linux, macOS, or Unix

Hay dos formas de conectarse a la interfaz de SMTP de Amazon SES con OpenSSL: mediante SSL explícito a través del puerto 587 o mediante SSL implícito a través del puerto 465.

Para conectarse a la interfaz SMTP mediante SSL explícito

- En la línea de comandos, ingrese el comando siguiente para conectarse al servidor SMTP de Amazon SES:

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

En el comando anterior, sustituya *email-smtp.us-west-2.amazonaws.com* por la URL del punto de enlace SMTP de Amazon SES de su AWS región. Para obtener más información, consulte the section called “Regiones”.

Si la conexión se realiza correctamente, aparece un resultado similar al siguiente:

```
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 conexión se cierra automáticamente después de unos 10 segundos de inactividad.

Como alternativa, puede utilizar SSL implícito para conectarse a la interfaz SMTP a través del puerto 465.

Para conectarse a la interfaz SMTP mediante SSL implícito

- En la línea de comandos, ingrese el comando siguiente para conectarse al servidor SMTP de Amazon SES:

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

En el comando anterior, sustituya *email-smtp.us-west-2.amazonaws.com* por la URL del punto de enlace SMTP de Amazon SES de su AWS región. Para obtener más información, consulte the section called “Regiones”.

Si la conexión se realiza correctamente, aparece un resultado similar al siguiente:

```
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 conexión se cierra automáticamente después de unos 10 segundos de inactividad.

PowerShell

Puede usar el NetConnection cmdlet Test- PowerShell para conectarse al servidor SMTP de Amazon SES.

> **Note**
>
> El cmdlet `Test-NetConnection` puede determinar si la computadora puede conectarse al punto de enlace de SMTP de Amazon SES. Sin embargo, no comprueba si el equipo puede realizar una conexión SSL implícita o explícita al punto de enlace SMTP. Para probar una conexión SSL, puede instalar OpenSSL para Windows para enviar un correo electrónico de prueba.

Para conectarse a la interfaz SMTP mediante el cmdlet **`Test-NetConnection`**

- En PowerShell, introduzca el siguiente comando para conectarse al servidor SMTP de Amazon SES:

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

En el comando anterior, sustituya *email-smtp.us-west-2.amazonaws.com* por la URL del punto de enlace SMTP de Amazon SES de su AWS región y sustituya *587* por el número de puerto. Para obtener más información acerca de los puntos de enlace regionales de Amazon SES, consulte the section called “Regiones”.

Si la conexión se ha realizado correctamente, verá un resultado similar al siguiente ejemplo:

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

Uso de la API de Amazon SES para enviar correo electrónico

Para enviar email de producción a través de Amazon SES, puede utilizar la interfaz de Simple Mail Transfer Protocol (SMTP) o la API de Amazon SES. Para obtener más información sobre la interfaz de SMTP, consulte Uso de la interfaz de SMTP de Amazon SES para enviar correo electrónico. Esta sección describe cómo enviar correo electrónico utilizando la API.

Cuando envía un correo electrónico mediante la API de Amazon SES, se especifica el contenido del mensaje y Amazon SES crea un correo electrónico MIME. También puede ensamblar el correo electrónico usted mismo para tener control total sobre el contenido del mensaje. Para obtener más información acerca del uso de la API de REST, consulte la Referencia de la API de Amazon Simple Email Service. Para obtener una lista de las direcciones URL de los puntos de conexión en los Regiones de AWS que Amazon SES está disponible, consulte los puntos de enlace y las cuotas de Amazon Simple Email Service en. Referencia general de AWS

Puede llamar al API de las formas siguientes:

- Realizar solicitudes HTTPS directas: este es el método más avanzado, ya que debe administrar manualmente la autenticación y la firma de sus solicitudes y, a continuación, crear las solicitudes de forma manual. Para obtener información acerca de la API de Amazon SES, consulte la página Bienvenido en la Referencia de la API v2.
- Utilice un AWS SDK:AWS los SDK facilitan el acceso a las API de varios AWS servicios, incluido Amazon SES. Cuando utiliza un SDK, se encarga de la autenticación, la firma de solicitudes, la

lógica de reintentos, el control de errores y otras funciones de bajo nivel para que pueda centrarse en crear aplicaciones que satisfagan a sus clientes.

- Utilizar una interfaz de línea de comandos: la AWS Command Line Interface es la herramienta de línea de comandos para Amazon SES. También ofrecemos las AWS herramientas PowerShell para quienes escriben en el PowerShell entorno.

Independientemente de si accede a la API de Amazon SES directa o indirectamente a través de un AWS SDK, AWS Command Line Interface o las AWS herramientas para PowerShell, la API de Amazon SES le ofrece dos formas diferentes de enviar un correo electrónico, según el grado de control que desee sobre la composición del mensaje de correo electrónico:

- Formateado: Amazon SES compone y envía un mensaje de correo electrónico con el formato adecuado. Solo hay que suministrar las direcciones “From:” (De:) y “To:” (Para:), un asunto y el cuerpo del mensaje. Amazon SES se encarga de todo lo demás. Para obtener más información, consulte Envío de correo electrónico con formato mediante la API de Amazon SES.
- Sin procesar: puede componer manualmente y enviar un mensaje de correo electrónico, especificando sus propios encabezados de correo electrónico y tipos de MIME. Si tiene experiencia en dar formato a su propio correo electrónico, esta interfaz le ofrece un mayor control sobre la composición del mensaje. Para obtener más información, consulte Envío de correo electrónico sin procesar mediante la API v2 de Amazon SES.

Contenido

- Envío de correo electrónico con formato mediante la API de Amazon SES
- Envío de correo electrónico sin procesar mediante la API v2 de Amazon SES
- Uso de plantillas para el envío de correo electrónico personalizado con la API de Amazon SES
- Envío de correo electrónico a través de Amazon SES mediante un AWS SDK
- Codificaciones de contenido compatibles con Amazon SES

Envío de correo electrónico con formato mediante la API de Amazon SES

Puede enviar un correo electrónico formateado utilizando AWS Management Console o llamando a la API de Amazon SES a través de una aplicación directamente, o indirectamente a través de un AWS SDK AWS Command Line Interface, el o el AWS Tools for Windows PowerShell.

La API de Amazon SES proporciona la acción `SendEmail`, que le permite componer y enviar un email con formato. `SendEmail` requiere una dirección de remitente "From:", una dirección de destinatario "To:", un asunto de mensaje y un cuerpo de mensaje (texto, HTML o ambos). Para obtener más información, consulte SendEmail(Referencia de la API) o SendEmail(Referencia de la API v2).

> **Note**
>
> La cadena de la dirección de correo electrónico debe ser un ASCII de 7 bits. Si desea enviar a direcciones de correo electrónico que contengan caracteres Unicode en la parte de dominio de una dirección o bien desde ellas, debe cifrar el dominio utilizando Punycode. Para obtener más información, consulte RFC 3492.

Para obtener ejemplos sobre cómo componer un mensaje con formato utilizando varios lenguajes de programación, consulte Ejemplos de código.

Para obtener consejos sobre cómo incrementar la velocidad de envío de correo electrónico al realizar varias llamadas a `SendEmail`, consulte Aumento del rendimiento con Amazon SES.

Envío de correo electrónico sin procesar mediante la API v2 de Amazon SES

Puede utilizar la `SendEmail` operación Amazon SES API v2 con el tipo de contenido especificado `raw` para enviar mensajes personalizados a sus destinatarios utilizando el formato de correo electrónico sin procesar.

Acerca de los campos de encabezados de correo electrónico

Simple Mail Transfer Protocol (SMTP) especifica la forma en que se envían los mensajes de correo electrónico definiendo el sobre del correo y algunos de sus parámetros, pero no se preocupa del contenido del mensaje. En lugar de ello, el formato de mensajes de Internet (RFC 5322) define cómo se construye el mensaje.

Con la especificación de formato de mensajes de Internet, todos los mensajes de correo electrónico se componen de un encabezado y de un cuerpo. El encabezado se compone de metadatos de mensaje y el cuerpo contiene el mensaje propiamente dicho. Para obtener más información acerca los encabezados y cuerpos de correo electrónico, consulte Formato de correo electrónico y Amazon SES.

Uso de MIME

El protocolo SMTP fue diseñado originalmente para enviar mensajes de correo electrónico que solo contenían caracteres ASCII de 7 bits. Esta especificación hace que SMTP no sea suficiente para codificaciones de texto no ASCII (como Unicode), contenido binario o archivos adjuntos. El estándar Multipurpose Internet Mail Extensions (MIME) se ha desarrollado para poder enviar muchas otras clases de contenido utilizando SMTP.

El estándar MIME funciona desglosando el cuerpo del mensaje en varias partes y, a continuación, especificando lo que hay que hacer con cada parte. Por ejemplo, una parte del cuerpo de un mensaje de correo electrónico podría ser texto sin formato, mientras que otra podría ser HTML. Además, MIME permite a los mensajes de correo electrónico contener uno o más archivos adjuntos. Los destinatarios del mensaje pueden ver los archivos adjuntos desde sus clientes de correo electrónico o pueden guardar los archivos adjuntos.

El encabezado del mensaje y el contenido están separados por una línea en blanco. Cada parte del correo electrónico está separada por un límite, una cadena de caracteres que indica el inicio y el final de cada parte.

El mensaje multiparte del siguiente ejemplo contiene un texto y una parte HTML y un archivo adjunto. El archivo adjunto se debe colocar justo debajo de los encabezados de archivo adjunto y, por lo general, se codifica en `base64` como se muestra en este ejemplo.

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

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

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

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

--sub_a3f166a86b56ff6c37755292d690675717ea3cd9de81228ec2b76ed4a15d6d1a
Content-Type: text/html; charset=iso-8859-1
```

```
Content-Transfer-Encoding: quoted-printable

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

--sub_a3f166a86b56ff6c37755292d690675717ea3cd9de81228ec2b76ed4a15d6d1a--

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

SUQsRmlyc3ROYW1lLExhc3ROYW1lLENvdW50cnkKMzQ4LEpvaG4sU3RpbGVzLENhbmFkYQo5MjM4
OSxKaWUsTGl1LENoaW5hCjczNCxTaGlybGV5LFJvZHJpZ3VleixVbml0ZWQgU3RhdGVzCjI4OTMs
QW5heWEsSXllbmdhcixJbmRpYQ==

--a3f166a86b56ff6c37755292d690675717ea3cd9de81228ec2b76ed4a15d6d1a--
```

El tipo de contenido del mensaje es `multipart/mixed`, lo que indica que el mensaje tiene muchas partes (en este ejemplo, un cuerpo y un archivo adjunto) y el cliente de recepción debe gestionar cada parte por separado.

Anidada en la sección del cuerpo, hay una segunda parte que utiliza el tipo de contenido `multipart/alternative`. Este tipo de contenido indica que cada parte contiene otras versiones alternativas del mismo contenido (en este caso, una versión de texto y una versión en HTML). Si el cliente de correo electrónico del destinatario puede mostrar contenido HTML, muestra la versión HTML del cuerpo del mensaje. Si el cliente de correo electrónico del destinatario no puede mostrar contenido HTML, muestra la versión de texto sin formato del cuerpo del mensaje.

Ambas versiones del mensaje también contendrán un archivo adjunto (en este caso, un archivo de texto breve que contiene los nombres de algunos clientes).

Al anidar una parte de MIME dentro de otra parte, como en este ejemplo, la parte anidada debe utilizar un parámetro `boundary` que es distinto del parámetro `boundary` en la parte principal. Estos límites deben ser cadenas de caracteres únicas. Para definir un límite entre las partes de MIME,

escriba dos guiones (--) seguidos de la cadena límite. Al final de una parte MIME, coloque dos guiones tanto al comienzo como al final de la cadena límite.

> **Note**
>
> Un mensaje no puede tener más de 500 partes MIME.

Codificación MIME

Para mantener la compatibilidad con sistemas antiguos, Amazon SES respeta la limitación de ASCII de 7 bits de SMTP, tal y como se define en RFC 2821. Si desea enviar contenido que contiene caracteres no ASCII, debe codificar los caracteres en un formato que utiliza caracteres ASCII de 7 bits.

Direcciones de correo electrónico

La cadena de la dirección de correo electrónico debe ser un ASCII de 7 bits. Si desea enviar a direcciones de correo electrónico que contengan caracteres Unicode en la parte de dominio de una dirección o bien desde ellas, debe cifrar el dominio utilizando Punycode. Punycode no se permite en la parte local de la dirección de correo electrónico (la parte delante del signo @) ni en el nombre de "remitente descriptivo". Si desea utilizar caracteres Unicode en el nombre de "remitente descriptivo", debe codificar el nombre de "remitente descriptivo" utilizando la sintaxis de palabra cifrada MIME, tal y como se describe en Envío de correo electrónico sin procesar mediante la API v2 de Amazon SES. Para obtener más información acerca de Punycode, consulte RFC 3492.

> **Note**
>
> Esta regla solo se aplica a las direcciones de correo electrónico que se especifican en el sobre, no a los encabezados del mensaje. Cuando utiliza la `SendEmail` operación Amazon SES API v2, las direcciones que especifique en `Destinations` los parámetros `Source` y definen el remitente y los destinatarios del sobre, respectivamente.

Encabezados de correo electrónico

Para codificar el encabezado de un mensaje, utilice la sintaxis de palabras codificadas de MIME. la sintaxis de palabras codificadas de MIME utiliza el formato siguiente:

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

El valor de *encoding* puede ser Q o B. Si el valor de encoding es Q, el valor *encoded-text* debe utilizar la codificación Q. Si el valor de encoding es B, el valor *encoded-text* debe utilizar la codificación Base64.

Por ejemplo, si desea utilizar la cadena “Як ти поживаєш?” en la línea de asunto de un correo electrónico, puede utilizar cualquiera de las siguientes codificaciones:

- Codificación Q

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

- Codificación Base64

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

Para obtener más información sobre la codificación Q, consulte RFC 2047. Para obtener más información sobre la codificación Base64, consulte RFC 2045.

Cuerpo del mensaje

Para codificar el cuerpo de un mensaje, puede utilizar la codificación quoted-printable o la codificación Base64. A continuación, utilice el encabezado `Content-Transfer-Encoding` para indicar el esquema de codificación que ha utilizado.

Por ejemplo, supongamos que el cuerpo del mensaje contiene el texto siguiente:

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

Si opta por codificar este texto con la codificación Base64, en primer lugar, especifique el siguiente encabezado:

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

A continuación, en la sección del cuerpo del mensaje, incluya el texto codificado en Base64:

```
4KWn4KWv4KWt4KWoIOCkruClhyDgpLDgpYcg4KSf4KWJ4KSu4KSy4KS/4KSC4KS44KSoIOCkqOCl
hyDgpKrgpLngpLLgpL4g4KSILeCkruClh+CksiDgpLjgpILgpKbgpYfgpLYg4KSt4KWH4KSc4KS+
IHwg4KSw4KWHIOCkn+ClieCkruCksuCkv+CkguCkuOCkqCDgpKjgpYcg4KS54KWAIOCkuOCksOCl
jeCkteCkquCljeCksOCkpeCkriBAIOCkmuCkv+CkqOCljeCkuSDgpJXgpL4g4KSa4KSv4KSoIOCk
leCkv+Ckr+CkviDgpJTgpLAg4KSH4KSo4KWN4KS54KWAIOCkleCliyDgpIjgpK7gpYfgpLIg4KSV
4KS+IOCkhuCkteCkv+Ckt+CljeCkleCkvuCksOCklSDgpK7gpL7gpKjgpL4g4KSc4KS+4KSk4KS+
IOCkueCliAo=
```

> **Note**
>
> En algunos casos, puede utilizar la `Content-Transfer-Encoding` de 8 bits en los mensajes que envíe a través de Amazon SES. Sin embargo, si Amazon SES tiene que realizar algún cambio en los mensajes (por ejemplo, cuando se utiliza el seguimiento de apertura y de clics), el contenido codificado en 8 bits podría no aparecer correctamente cuando llegue a las bandejas de correo de los destinatarios. Por este motivo, siempre debe codificar el contenido que no esté en ASCII de 7 bits.

Archivos adjuntos

Para adjuntar un archivo a un correo electrónico, debe codificar el archivo adjunto con la codificación Base64. Los archivos adjuntos normalmente se colocan en partes de mensaje MIME dedicadas, que incluyen los siguientes encabezados:

- Tipo de contenido: el tipo de archivo del archivo adjunto. A continuación, se muestran ejemplos de declaraciones comunes de Content-Type de MIME:
  - Archivo de texto sin formato: `Content-Type: text/plain; name="sample.txt"`
  - Documento de Microsoft Word: `Content-Type: application/msword; name="document.docx"`
  - Imagen JPG: `Content-Type: image/jpeg; name="photo.jpeg"`
- Disposición de contenido: especifica cómo debe gestionar el contenido el cliente de correo electrónico del destinatario. Para los archivos adjuntos, este valor es `Content-Disposition: attachment`.
- Codificación de transferencia de contenido: el esquema que se utilizó para codificar el archivo adjunto. Para los archivos adjuntos, este valor casi siempre es `base64`.
- El archivo adjunto codificado: debe codificar el archivo adjunto real e incluirlo en el cuerpo, debajo de los encabezados de archivo adjunto, como se muestra en el ejemplo.

Amazon SES acepta los tipos de archivos más comunes. Para obtener una lista de los tipos de archivos que Amazon SES no acepta, consulte Tipos de adjuntos no compatibles con Amazon SES.

Envío de correo electrónico sin procesar mediante la API v2 de Amazon SES

La API v2 de Amazon SES proporciona la `SendEmail` acción, que le permite redactar y enviar un mensaje de correo electrónico en el formato que especifique al configurar el tipo de contenido como simple, sin procesar o con plantillas. Para obtener una descripción completa, consulte `SendEmail`. El siguiente ejemplo especificará el tipo de contenido `raw` para enviar un mensaje utilizando el formato de correo electrónico sin procesar.

> **Note**
>
> Para obtener consejos sobre cómo incrementar la velocidad de envío de correo electrónico al realizar varias llamadas a `SendEmail`, consulte Aumento del rendimiento con Amazon SES.

El cuerpo del mensaje debe contener un mensaje de correo electrónico sin procesar con el formato correcto, con campos de encabezado adecuados y con codificación del cuerpo del mensaje. Aunque es posible construir el mensaje sin procesar manualmente dentro de una aplicación, es mucho más sencillo hacerlo a través de las bibliotecas de correo existentes.

Java

El siguiente ejemplo de código muestra cómo utilizar la JavaMailbiblioteca y la AWS SDK for Javapara redactar y enviar un correo electrónico sin procesar.

```
package com.amazonaws.samples;

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

// JavaMail libraries. Download the JavaMail API
// from https://javaee.github.io/javamail/
import javax.activation.DataHandler;
import javax.activation.DataSource;
import javax.activation.FileDataSource;
import javax.mail.Message;
```

```
import javax.mail.MessagingException;
import javax.mail.Session;
import javax.mail.internet.AddressException;
import javax.mail.internet.InternetAddress;
import javax.mail.internet.MimeBodyPart;
import javax.mail.internet.MimeMessage;
import javax.mail.internet.MimeMultipart;

// AWS SDK libraries. Download the AWS SDK for Java // from https://aws.amazon.com/
sdk-for-java
import com.amazonaws.regions.Regions;
import com.amazonaws.services.simpleemail.AmazonSimpleEmailService;
import com.amazonaws.services.simpleemail.AmazonSimpleEmailServiceClientBuilder;
import com.amazonaws.services.simpleemail.model.RawMessage;
import com.amazonaws.services.simpleemail.model.SendRawEmailRequest;

public class AmazonSESSample {

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

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

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

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

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

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

 // The HTML body of the email.
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

        // Define the attachment
        MimeBodyPart att = new MimeBodyPart();
        DataSource fds = new FileDataSource(ATTACHMENT);
        att.setDataHandler(new DataHandler(fds));
        att.setFileName(fds.getName());

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

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

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

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

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

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

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

Python

El siguiente ejemplo de código muestra cómo utilizar los paquetes email.mime de Python y el AWS SDK for Python (Boto) para componer y enviar un correo electrónico sin procesar.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# Define the attachment part and encode it using MIMEApplication.
```

```
att = MIMEApplication(open(ATTACHMENT, 'rb').read())

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

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

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

Uso de plantillas para el envío de correo electrónico personalizado con la API de Amazon SES

Puede utilizar la operación de la CreateTemplateAPI para crear plantillas de correo electrónico. Estas plantillas incluyen una línea de asunto y el texto y partes en HTML del cuerpo del correo electrónico. Las secciones de asunto y cuerpo también podrían contener valores únicos personalizados para cada destinatario.

Existen unos límites y otras consideraciones al utilizar estas características:

- Puedes crear hasta 20 000 plantillas de correo electrónico en cada una Región de AWS.
- Cada plantilla puede tener un tamaño de hasta 500 KB, incluidos el texto y las partes en HTML.
- Puede incluir un número ilimitado de variables de sustitución en cada plantilla.
- Puede enviar correo electrónico a un máximo de 50 destinos en cada llamada a la operación `SendBulkTemplatedEmail`. Un destino incluye una lista de destinatarios, así como los destinatarios CC y BCC. El número de destinos con los que puede ponerse en contacto en una única llamada a la API podría estar limitado por la tasa de envío máxima de su cuenta. Para obtener más información, consulte Administración de sus límites de envío de Amazon SES.

Esta sección incluye procedimientos para la creación de plantillas de correo electrónico y para el envío de correos electrónicos personalizados.

> **Note**
>
> En los procedimientos que se describen en esta sección, se da por hecho que ya se ha instalado y configurado la AWS CLI. Para obtener más información sobre la instalación y configuración de AWS CLI, consulte la Guía del AWS Command Line Interface usuario.

Parte 1: Configurar las notificaciones de eventos de errores de presentación

Si envía un correo electrónico que contiene contenido de personalización no válido, Amazon SES puede aceptar inicialmente el mensaje, pero puede no ser capaz de enviarlo. Por este motivo, si tiene previsto enviar correo electrónico personalizado, debe configurar Amazon SES para enviar notificaciones de eventos de errores de presentación a través de Amazon SNS. Cuando reciba una notificación de evento de error de presentación, puede identificar qué mensaje incluía el contenido no válido, solucionar los problemas y enviar el mensaje de nuevo.

Es absolutamente recomendable que realice el procedimiento de esta sección, aunque sea opcional.

Para configurar notificaciones de eventos de errores de presentación

1. Cree un tema de Amazon SNS. Para obtener información acerca de los procedimientos, consulte Creación de un tema en la Guía para desarrolladores de Amazon Simple Notification Service.

2. Suscríbase al tema de Amazon SNS. Por ejemplo, si desea recibir notificaciones de errores de presentación por correo electrónico, suscriba un punto de enlace de correo electrónico (es decir, su dirección de correo electrónico) al tema.

   Para obtener información acerca de los procedimientos, consulte Suscribirse a un tema en la Guía para desarrolladores de Amazon Simple Notification Service.

3. Realice los procedimientos de the section called “Configuración de un destino de Amazon SNS” para configurar los conjuntos de configuración con el objetivo de publicar eventos de errores de presentación en su tema de Amazon SNS.

Parte 2: Crear una plantilla de correo electrónico

En esta sección, se utiliza la operación de la CreateTemplate API para crear una nueva plantilla de correo electrónico con atributos de personalización.

En este procedimiento se presupone que ya ha instalado y configurado la AWS CLI. Para obtener más información sobre la instalación y configuración de AWS CLI, consulte la Guía del AWS Command Line Interface usuario.

Para crear la plantilla

1. En un editor de texto, cree un nuevo archivo. Pegue el código siguiente en el archivo.

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

   Este código contiene las siguientes propiedades:

   - TemplateName— El nombre de la plantilla. Cuando envíe el correo electrónico, consulte este nombre.

- SubjectPart— La línea de asunto del correo electrónico. Esta propiedad podría contener etiquetas de sustitución. Estas etiquetas utilizan el siguiente formato: `{{tagname}}`. Cuando envíe el correo electrónico, puede especificar un valor para `tagname` para cada destino.

  El ejemplo anterior incluye dos etiquetas: `{{name}}` y `{{favoriteanimal}}`.
- HtmlPart— El cuerpo HTML del correo electrónico. Esta propiedad podría contener etiquetas de sustitución.
- TextPart— El cuerpo del texto del correo electrónico. Los destinatarios cuyos clientes de correo electrónico no muestran el correo electrónico en HTML ven esta versión del correo electrónico. Esta propiedad podría contener etiquetas de sustitución.

2. Personalice el ejemplo anterior para adaptarse a sus necesidades y, a continuación, guarde el archivo como `mytemplate.json`.
3. En la línea de comandos, escriba el siguiente comando para crear una nueva plantilla utilizando la operación `CreateTemplate` de la API:

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

Parte 3: Enviar el correo electrónico personalizado

Después de crear una plantilla de correo electrónico, puede utilizarla para enviar correo electrónico. Existen dos operaciones de la API que puede utilizar para enviar mensajes de correo utilizando plantillas: `SendTemplatedEmail` y `SendBulkTemplatedEmail`. La operación `SendTemplatedEmail` resulta útil para enviar un correo electrónico personalizado a un único destino (una colección de destinatarios "To", "CC" y "BCC" que recibirán el mismo correo electrónico). La operación `SendBulkTemplatedEmail` resulta útil para enviar correos electrónicos únicos a varios destinos en una única llamada a la API de Amazon SES. En esta sección se proporcionan ejemplos de cómo utilizar el AWS CLI para enviar correos electrónicos mediante estas dos operaciones.

Envío de correo electrónico con plantilla a un destino único

Puede utilizar la operación `SendTemplatedEmail` para enviar un correo electrónico a un destino único. Todos los destinatarios del objeto `Destination` recibirán el mismo correo electrónico.

Para enviar un correo electrónico con plantilla a un destino único

1. En un editor de texto, cree un nuevo archivo. Pegue el código siguiente en el archivo.

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

Este código contiene las siguientes propiedades:

- Source: la dirección de correo electrónico del remitente.
- Template: el nombre de la plantilla que aplicar al correo electrónico.
- ConfigurationSetNombre: el nombre del conjunto de configuraciones que se utilizará al enviar el correo electrónico.

> **Note**
>
> Le recomendamos que utilice un conjunto de configuración que esté configurado para publicar eventos de errores de presentación en Amazon SNS. Para obtener más información, consulte the section called “Parte 1: Configurar las notificaciones”.

- Destination: las direcciones de destinatario. Puede incluir varias direcciones "To", "CC" y "BCC". Cuando utiliza la operación `SendTemplatedEmail`, todos los destinatarios reciben el mismo mensaje de correo electrónico.
- TemplateData— Una cadena JSON de escape que contiene pares clave-valor. Las claves corresponden a las variables de la plantilla (por ejemplo, `{{name}}`). Los valores representan el contenido que sustituye las variables en el correo electrónico.

2. Cambie los valores del código del paso anterior según sus necesidades y, a continuación, guarde el archivo como `myemail.json`.
3. En la línea de comandos, escriba el siguiente comando para enviar el correo electrónico:

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

Envío de correo electrónico con plantilla a varios destinos

Puede utilizar la operación `SendBulkTemplatedEmail` para enviar un correo electrónico a varios destinos en una llamada única al API. Amazon SES envía un correo electrónico único al destinatario o destinatarios en cada objeto `Destination`.

Para enviar un correo electrónico con plantilla a varios destinos

1. En un editor de texto, cree un nuevo archivo. Pegue el código siguiente en el archivo.

```
{
  "Source":"Mary Major <mary.major@example.com>",
  "Template":"MyTemplate",
  "ConfigurationSetName": "ConfigSet",
  "Destinations":[
    {
      "Destination":{
        "ToAddresses":[
          "anaya.iyengar@example.com"
        ]
      },
      "ReplacementTemplateData":"{ \"name\":\"Anaya\", \"favoriteanimal\":
\"angelfish\" }"
    },
    {
      "Destination":{
        "ToAddresses":[
          "liu.jie@example.com"
        ]
      },
      "ReplacementTemplateData":"{ \"name\":\"Liu\", \"favoriteanimal\":\"lion\" }"
    },
    {
      "Destination":{
        "ToAddresses":[
          "shirley.rodriguez@example.com"
        ]
      },
      "ReplacementTemplateData":"{ \"name\":\"Shirley\", \"favoriteanimal\":\"shark
\" }"
    },
    {
      "Destination":{
```

```
        "ToAddresses":[
          "richard.roe@example.com"
        ]
      },
      "ReplacementTemplateData":"{}"
    }
  ],
  "DefaultTemplateData":"{ \"name\":\"friend\", \"favoriteanimal\":\"unknown\" }"
}
```

Este código contiene las siguientes propiedades:

- Source: la dirección de correo electrónico del remitente.
- Template: el nombre de la plantilla que aplicar al correo electrónico.
- ConfigurationSetNombre: el nombre del conjunto de configuraciones que se utilizará al enviar el correo electrónico.

> **Note**
>
> Le recomendamos que utilice un conjunto de configuración que esté configurado para publicar eventos de errores de presentación en Amazon SNS. Para obtener más información, consulte the section called “Parte 1: Configurar las notificaciones”.

- Destinos: una matriz que contiene uno o varios destinos.
  - Destination: las direcciones de destinatario. Puede incluir varias direcciones "To", "CC" y "BCC". Cuando utiliza la operación `SendBulkTemplatedEmail`, todos los destinatarios dentro del mismo objeto `Destination` reciben el mismo mensaje de correo electrónico.
  - ReplacementTemplateDatos: objeto JSON que contiene pares clave-valor. Las claves corresponden a las variables de la plantilla (por ejemplo, `{{name}}`). Los valores representan el contenido que sustituye las variables en el correo electrónico.
- DefaultTemplateDatos: objeto JSON que contiene pares clave-valor. Las claves corresponden a las variables de la plantilla (por ejemplo, `{{name}}`). Los valores representan el contenido que sustituye las variables en el correo electrónico. Esta objeto contiene datos alternativos. Si un objeto `Destination` contiene un objeto JSON vacío en la propiedad `ReplacementTemplateData`, se utilizan los valores de la propiedad `DefaultTemplateData`.

2. Cambie los valores del código del paso anterior según sus necesidades y, a continuación, guarde el archivo como `mybulkemail.json`.
3. En la línea de comandos, escriba el siguiente comando para enviar el correo masivo:

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

Personalización avanzada del correo electrónico

La característica de plantillas de Amazon SES se basa en el sistema de plantillas de Handlebars. Puede utilizar Handlebars para crear plantillas que incluyan características avanzadas, como atributos anidados, iteración de matrices, instrucciones condicionales básicas y la creación de funciones parciales insertadas. En esta sección se proporcionan ejemplos de estas características.

Handlebars incluye características adicionales además de las documentadas en esta sección. Para obtener más información, consulte Built-In Helpers en handlebarsjs.com.

> **Note**
>
> SES no aplica secuencias de escape al contenido HTML cuando renderiza la plantilla HTML de un mensaje. Esto significa que si incluye datos introducidos por el usuario, como desde un formulario de contacto, tendrá que aplicar las secuencias de escape en el lado del cliente.

Temas

- Análisis de atributos anidados
- Recorrido de listas en iteración
- Uso de instrucciones condicionales básicas
- Creación de funciones parciales insertadas

Análisis de atributos anidados

Handlebars admite rutas anidadas, lo que facilita la organización de datos de clientes complejos y la referencia a esos datos en sus plantillas de correo electrónico.

Por ejemplo, puede organizar los datos de los destinatarios en varias categorías generales. Dentro de cada una de estas categorías, puede incluir información detallada. El siguiente ejemplo de código muestra un ejemplo de esta estructura para un único destinatario:

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

En sus plantillas de correo electrónico, puede hacer referencia a atributos anidados proporcionando el nombre del atributo principal, seguido de un punto (.), seguido del nombre del atributo para el que desea incluir el valor. Por ejemplo, si utiliza la estructura de datos que se muestra en el ejemplo anterior y desea incluir el nombre de cada destinatario en la plantilla de correo electrónico, incluya el siguiente texto en su plantilla de correo electrónico: `Hello {{contact.firstName}}!`

Handlebars puede analizar rutas que tengan varios niveles anidados, lo que le proporciona flexibilidad a la hora de estructurar los datos de la plantilla.

Recorrido de listas en iteración

La función auxiliar `each` recorre en iteración los elementos de una matriz. El código siguiente es un ejemplo de una plantilla de correo electrónico que utiliza la función auxiliar `each` para crear una relación detallada de los intereses de cada destinatario.

```
{
  "Template": {
    "TemplateName": "Preferences",
```

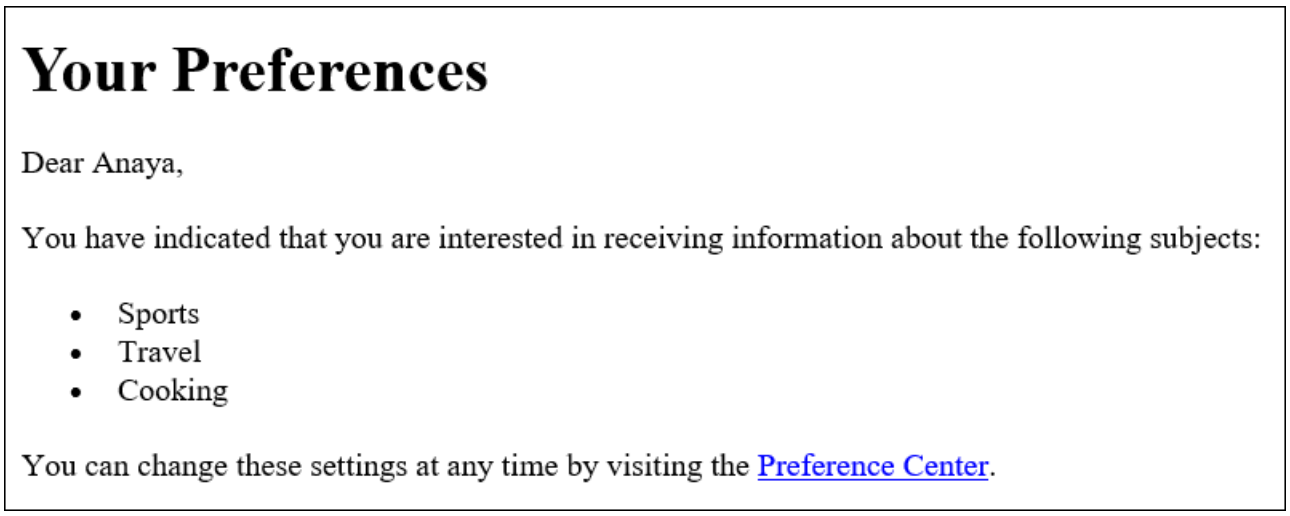
```
    "SubjectPart": "Subscription Preferences for {{contact.firstName}}
 {{contact.lastName}}",
    "HtmlPart": "<h1>Your Preferences</h1>
                <p>You have indicated that you are interested in receiving
                  information about the following subjects:</p>
                <ul>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

> **Important**
>
> En el ejemplo de código anterior, los valores de los atributos `HtmlPart` y `TextPart` incluyen saltos de línea para facilitar la lectura del ejemplo. El archivo JSON de la plantilla no puede contener saltos de línea dentro de estos valores. Si ha copiado y pegado este ejemplo en su propio archivo JSON, elimine los saltos de línea y espacios adicionales de las secciones `HtmlPart` y `TextPart` antes de continuar.

Después de crear la plantilla, puede utilizar la operación `SendTemplatedEmail` o `SendBulkTemplatedEmail` para enviar correo electrónico a los destinatarios a través de esta plantilla. Siempre y cuando los destinatarios tengan al menos un valor en el objeto `Interests`, reciben un correo electrónico que incluye una relación detallada de sus intereses. El siguiente ejemplo muestra un archivo JSON que se puede utilizar para enviar correo electrónico a varios destinatarios mediante la plantilla anterior:

```
{
  "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\":[]}"
}
```

Cuando envíe un correo electrónico a los destinatarios indicados en el ejemplo anterior mediante la operación `SendBulkTemplatedEmail`, recibirán un mensaje similar al ejemplo que se muestra en la siguiente imagen:



Uso de instrucciones condicionales básicas

Esta sección se basa en el ejemplo descrito en la sección anterior. El ejemplo de la sección anterior utiliza la función auxiliar `each` para recorrer en iteración una lista de intereses. Sin embargo, los destinatarios para los que no se especifican intereses reciben un correo electrónico que contiene una lista vacía. Mediante la función auxiliar `{{if}}`, puede formatear el correo electrónico de forma distinta si un determinado atributo está presente en la plantilla de datos. El código siguiente utiliza la función auxiliar `{{if}}` para mostrar la lista con viñetas de la sección anterior si la matriz `Subscription` contiene algún valor. Si la matriz está vacía, se muestra un bloque de texto diferente.

```
{
  "Template": {
    "TemplateName": "Preferences2",
    "SubjectPart": "Subscription Preferences for {{contact.firstName}}
 {{contact.lastName}}",
    "HtmlPart": "<h1>Your Preferences</h1>
                <p>Dear {{contact.firstName}},</p>
                {{#if subscription}}
                  <p>You have indicated that you are interested in receiving
                    information about the following subjects:</p>
                    <ul>
                    {{#each subscription}}
                      <li>{{interest}}</li>
                    {{/each}}
                    </ul>
                    <p>You can change these settings at any time by visiting
```

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

> **Important**
>
> En el ejemplo de código anterior, los valores de los atributos `HtmlPart` y `TextPart` incluyen saltos de línea para facilitar la lectura del ejemplo. El archivo JSON de la plantilla no puede contener saltos de línea dentro de estos valores. Si ha copiado y pegado este ejemplo en su propio archivo JSON, elimine los saltos de línea y espacios adicionales de las secciones `HtmlPart` y `TextPart` antes de continuar.

El siguiente ejemplo muestra un archivo JSON que se puede utilizar para enviar correo electrónico a varios destinatarios mediante la plantilla anterior:

```
{
  "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\":[]}"
}
```

En este ejemplo, el destinatario cuyos datos de la plantilla incluyen una lista de intereses recibe el mismo correo electrónico que el ejemplo mostrado en la sección anterior. Sin embargo, el destinatario cuyos datos de la plantilla no incluyen intereses, recibe un correo electrónico similar al ejemplo que se muestra en la siguiente imagen:

Creación de funciones parciales insertadas

Puede utilizar funciones parciales insertadas para simplificar las plantillas que incluyen cadenas repetidas. Por ejemplo, podría crear una función parcial insertada que incluyera el nombre del destinatario y, si está disponible, sus apellidos agregando el siguiente código al principio de la plantilla:

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

> **Note**
>
> El carácter de nueva línea (\n) es necesario para separar el bloque `{{inline}}` del contenido de la plantilla. La nueva línea no se muestra en el resultado final.

Después de crear la función parcial `fullName`, puede incluirla en cualquier lugar de la plantilla añadiendo delante del nombre de la función parcial un signo mayor que (>) seguido de un espacio, como en el siguiente ejemplo: `{{> fullName}}`. Las funciones parciales insertadas no se transfieren entre las distintas partes del correo electrónico. Por ejemplo, si desea utilizar la misma función parcial insertada en la versión HTML y de texto del correo electrónico, debe definirla en las secciones `HtmlPart` y `TextPart`.

También puede utilizar funciones parciales insertadas cuando recorre en iteración matrices. Puede utilizar el siguiente código para crear una plantilla que utilice la función parcial insertada `fullName`. En este ejemplo, la función parcial insertada se aplica tanto al nombre del destinatario como a una matriz de otros nombres:

```
{
  "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**
>
> En el ejemplo de código anterior, los valores de los atributos `HtmlPart` y `TextPart` incluyen saltos de línea para facilitar la lectura del ejemplo. El archivo JSON de la plantilla no puede contener saltos de línea dentro de estos valores. Si ha copiado y pegado este ejemplo en su propio archivo JSON, elimine los saltos de línea y espacios adicionales de estas secciones.

Administración de plantillas de correo electrónico

Además de crear de plantillas de correo electrónico, también puede utilizar la API de Amazon SES para actualizar o eliminar plantillas existentes, enumerar todas las plantillas existentes o ver el contenido de una plantilla.

Esta sección contiene los procedimientos para utilizarlos AWS CLI para realizar tareas relacionadas con las plantillas de Amazon SES.

> **Note**
>
> En los procedimientos que se describen en esta sección, se da por hecho que ya se ha instalado y configurado la AWS CLI. Para obtener más información sobre la instalación y configuración de AWS CLI, consulte la Guía del AWS Command Line Interface usuario.

Visualización de una lista de plantillas de correo electrónico

Puede usar la ListTemplatesoperación en la API de Amazon SES para ver una lista de todas sus plantillas de correo electrónico existentes.

Para ver una lista de plantillas de correo electrónico

- En la línea de comandos, escriba el comando siguiente.

```
aws ses list-templates
```

Si hay plantillas de correo electrónico existentes en su cuenta de Amazon SES en la región actual, este comando devuelve una respuesta similar al siguiente ejemplo:

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

Si no ha creado ninguna plantilla, el comando devuelve un objeto `TemplatesMetadata` sin miembros.

Visualización del contenido de una plantilla de correo electrónico específica

Puede usar la GetTemplateoperación en la API de Amazon SES para ver el contenido de una plantilla de correo electrónico específica.

Para ver el contenido de una plantilla de correo electrónico

- En la línea de comandos, escriba el comando siguiente.

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

En el comando anterior, *MyTemplate*sustitúyalo por el nombre de la plantilla que desea ver.

Si el nombre de la plantilla que ha proporcionado coincide con una plantilla existente en su cuenta de Amazon SES, este comando devuelve una respuesta similar al ejemplo siguiente:

```
{
    "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 el nombre de la plantilla que ha proporcionado no coincide con una plantilla existente en su cuenta de Amazon SES, el comando devuelve un error `TemplateDoesNotExist`.

Eliminación de una plantilla de correo electrónico

Puede utilizar la DeleteTemplateoperación de la API de Amazon SES para eliminar una plantilla de correo electrónico específica.

Para eliminar una plantilla de correo electrónico

- En la línea de comandos, escriba el comando siguiente.

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

En el comando anterior, *`MyTemplate`*sustitúyalo por el nombre de la plantilla que deseas eliminar.

Este comando no proporciona ningún resultado. Puede comprobar que la plantilla se ha eliminado mediante la GetTemplateoperación.

Actualización de una plantilla de correo electrónico

Puede utilizar la UpdateTemplateoperación de la API de Amazon SES para actualizar una plantilla de correo electrónico existente. Por ejemplo, esta operación es útil si desea cambiar la línea de asunto de la plantilla de correo electrónico o si necesita modificar el cuerpo del mensaje en sí.

Para actualizar una plantilla de correo electrónico

1. Utilice el comando `GetTemplate` para recuperar la plantilla existente al ingresar el siguiente comando en la línea de comandos:

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

En el comando anterior, *MyTemplate*sustitúyalo por el nombre de la plantilla que deseas actualizar.

Si el nombre de la plantilla que ha proporcionado coincide con una plantilla existente en su cuenta de Amazon SES, este comando devuelve una respuesta similar al ejemplo siguiente:

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

2. En un editor de texto, cree un nuevo archivo. Pegue el resultado del comando anterior en el archivo.
3. Modifique la plantilla como sea necesario. Las líneas que se omitan se eliminarán de la plantilla. Por ejemplo, si solo desea cambiar la `SubjectPart` de la plantilla, aún debe incluir las propiedades `TextPart` y `HtmlPart`.

   Cuando haya terminado, guarde el archivo como `update_template.json`.
4. En la línea de comandos, escriba el comando siguiente.

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

   En el comando anterior, reemplace *path/to/update_template.json* con la ruta al archivo `update_template.json` que ha creado en el paso anterior.

   Si la plantilla se actualiza correctamente, este comando no proporcionará ningún resultado. Puede comprobar que la plantilla se ha actualizado mediante la GetTemplateoperación.

   Si la plantilla especificada no existe, este comando devuelve un error `TemplateDoesNotExist`. Si la plantilla no contiene ninguna de las propiedades `TextPart` o `HtmlPart` (o ambas), este comando devuelve un error `InvalidParameterValue`.

Envío de correo electrónico a través de Amazon SES mediante un AWS SDK

Puede usar un AWS SDK para enviar correos electrónicos a través de Amazon SES. AWS Los SDK están disponibles para varios lenguajes de programación. Para obtener más información, consulte Herramientas para Amazon Web Services.

Requisitos previos

Se deben completar los siguientes requisitos previos para completar cualquiera de los ejemplos de código de la sección siguiente:

- Si aún no lo ha hecho, realice las tareas de Configuración de Amazon Simple Email Service.
- Verifique su dirección de correo electrónico con Amazon SES: para poder enviar correo electrónico con Amazon SES, debe verificar que es propietario de la dirección de correo electrónico del remitente. Si su cuenta aún está en el entorno de pruebas de Amazon SES, también tiene que verificar la dirección de correo electrónico del destinatario. Le recomendamos que utilice la consola de Amazon SES para verificar las direcciones de correo electrónico. Para obtener más información, consulte Creación de una identidad de dirección de correo electrónico.
- Obtenga sus AWS credenciales: necesita un identificador de clave de AWS acceso y una clave de acceso AWS secreta para acceder a Amazon SES mediante un SDK. Puede encontrar sus credenciales utilizando la página Security Credentials (Credenciales de seguridad) de la AWS Management Console. Para obtener más información acerca de las credenciales, consulte Tipos de credenciales de Amazon SES.
- Cree un archivo de credenciales compartidas: para que el código de muestra de esta sección funcione correctamente, debe crear un archivo de credenciales compartidas. Para obtener más información, consulte Crear un archivo de credenciales compartido para usarlo al enviar correos electrónicos a través de Amazon SES mediante un AWS SDK.

Ejemplos de código

> **Important**
>
> En los tutoriales siguientes, deberá enviarse un correo electrónico a usted mismo para poder verificar si lo recibe. Para seguir experimentando o realizar pruebas de carga, utilice el simulador de buzón de correo de Amazon SES. Los correos electrónicos que envíe al simulador de buzón de correo no se contabilizan en su cuota de envío ni en sus tasas de

rebotes y reclamos. Para obtener más información, consulte Uso del simulador de buzón de correo de forma manual.

.NET

El siguiente procedimiento muestra cómo enviar un correo electrónico a través de Amazon SES mediante Visual Studio y AWS SDK for .NET.

Esta solución se ha probado utilizando los siguientes componentes:

- Microsoft Visual Studio Community 2017, versión 15.4.0.
- Microsoft .NET Framework versión 4.6.1.
- El paquete AWSSDK .Core (versión 3.3.19), instalado mediante. NuGet
- AWSSDKEl. SimpleEmail paquete (versión 3.3.6.1), instalado usando. NuGet

Antes de empezar, lleva a cabo las tareas siguientes:

- Instale Visual Studio: Visual Studio está disponible en https://www.visualstudio.com/.

Para enviar un correo electrónico mediante el AWS SDK for .NET

1. Cree un proyecto nuevo realizando los pasos siguientes:
   a. Inicie Visual Studio.
   b. En el menú File (Archivo), elija New (Nuevo), Project (Proyecto).
   c. En la ventana New Project, en el panel de la izquierda, expanda Installed y, a continuación, expanda Visual C#.
   d. En el panel de la derecha, seleccione Console App (.NET Framework).
   e. En Name (Nombre), escriba **`AmazonSESSample`** y, a continuación, elija OK (Aceptar).
2. NuGet Úselos para incluir los paquetes de Amazon SES en su solución siguiendo los siguientes pasos:
   a. En el panel Explorador de soluciones, haga clic con el botón derecho en su proyecto y, a continuación, seleccione Administrar NuGet paquetes.
   b. En la pestaña NuGetAmazonsessSample, selecciona Browse.

c. En el campo de búsqueda, escriba **`AWSSDK.SimpleEmail`**.

d. Elija el. AWSSDK SimpleEmailpaquete y, a continuación, selecciona Instalar.

e. En la ventana Preview Changes, elija OK.

3. En la pestaña Program.cs, pegue el código siguiente:

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

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

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

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

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

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

        // The HTML body of the email.
        static readonly string htmlBody = @"<html>
<head></head>
<body>
```

```
  <h1>Amazon SES Test (AWS SDK for .NET)</h1>
  <p>This email was sent with
    <a href='https://aws.amazon.com/ses/'>Amazon SES</a> using the
    <a href='https://aws.amazon.com/sdk-for-net/'> AWS SDK for .NET</a>.</p>
</body>
</html>";

        static void Main(string[] args)
        {
            // Replace USWest2 with the AWS Region you're using for Amazon SES.
            // Acceptable values are EUWest1, USEast1, and USWest2.
            using (var client = new
 AmazonSimpleEmailServiceClient(RegionEndpoint.USWest2))
            {
                var sendRequest = new SendEmailRequest
                {
                    Source = senderAddress,
                    Destination = new Destination
                    {
                        ToAddresses =
                        new List<string> { receiverAddress }
                    },
                    Message = new Message
                    {
                        Subject = new Content(subject),
                        Body = new Body
                        {
                            Html = new Content
                            {
                                Charset = "UTF-8",
                                Data = htmlBody
                            },
                            Text = new Content
                            {
                                Charset = "UTF-8",
                                Data = textBody
                            }
                        }
                    },
                    // If you are not using a configuration set, comment
                    // or remove the following line
                    ConfigurationSetName = configSet
                };
                try
```

```
                {
                    Console.WriteLine("Sending email using Amazon SES...");
                    var response = client.SendEmail(sendRequest);
                    Console.WriteLine("The email was sent successfully.");
                }
                catch (Exception ex)
                {
                    Console.WriteLine("The email was not sent.");
                    Console.WriteLine("Error message: " + ex.Message);

                }
            }

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

4. En el editor de código, haga lo siguiente:

   - Reemplace *sender@example.com* por la dirección de correo electrónico del remitente. Esta dirección debe verificarse. Para obtener más información, consulte Identidades verificadas.
   - Reemplace *recipient@example.com* por la dirección de destino. Si su cuenta está todavía en el entorno de pruebas, esta dirección también se debe verificar.
   - *ConfigSet*Sustitúyalo por el nombre del conjunto de configuraciones que se utilizará al enviar este correo electrónico.
   - Sustituya *USWest2* por el nombre del Región de AWS punto de conexión que utiliza para enviar correos electrónicos mediante Amazon SES. Para ver una lista de las regiones donde Amazon SES está disponible, consulte Amazon Simple Email Service (Amazon SES) en la Referencia general de AWS.

   Cuando termine, guarde `Program.cs`.

5. Cree y ejecute la aplicación completando los pasos siguientes:

   a. En el menú Build, elija Build Solution.

   b. En el menú Debug, elija Start Debugging. Aparece una ventana de consola.

6. Revise la salida de la consola. Si el correo electrónico se envía correctamente, la consola muestra `The email was sent successfully.`
7. Si el correo electrónico se ha enviado correctamente, inicie sesión en el cliente de correo electrónico de la dirección del destinatario. Ahí podrá ver el mensaje que ha enviado.

Java

El siguiente procedimiento muestra cómo utilizar el IDE de Eclipse para desarrolladores de Java EE y cómo AWS Toolkit for Eclipsecrear un proyecto de AWS SDK y modificar el código de Java para enviar un correo electrónico a través de Amazon SES.

Antes de empezar, lleva a cabo las tareas siguientes:

- Instale Eclipse: Eclipse está disponible en https://www.eclipse.org/downloads. El código en este tutorial se ha probado mediante Eclipse Neon.3 (versión 4.6.3), ejecutando la versión 1.8 de Java Runtime Environment (JRE).
- Instale el AWS Toolkit for Eclipse: las instrucciones para añadirlo AWS Toolkit for Eclipse a su instalación de Eclipse están disponibles en https://aws.amazon.com/eclipse. El código de este tutorial se ha probado utilizando la versión 2.3.1 del AWS Toolkit for Eclipse.

Para enviar un correo electrónico utilizando el AWS SDK for Java

1. Cree un proyecto AWS Java en Eclipse realizando los siguientes pasos:
    a. Inicie Eclipse.
    b. En el menú File, elija New y, a continuación, elija Other. En la ventana New, expanda la carpeta AWS y, a continuación, elija AWS Java Project.
    c. En el cuadro de diálogo Nuevo proyecto AWS Java, haga lo siguiente:
        i. Para Project name, escriba un nombre de proyecto.
        ii. En AWS SDK for Java Ejemplos, selecciona Amazon Simple Email Service JavaMail Sample.
        iii. Seleccione Finalizar.
2. En Eclipse, en la página Package Explorer, amplíe su proyecto.

3. En su proyecto, expanda la carpeta `src/main/java`, la carpeta `com.amazon.aws.samples` y, a continuación, haga doble clic en `AmazonSESSample.java`.
4. Reemplace todo el contenido de `AmazonSESSample.java` por el siguiente código:

```
package com.amazonaws.samples;

import java.io.IOException;

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

public class AmazonSESSample {

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

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

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

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

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

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

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

    try {
      AmazonSimpleEmailService client =
          AmazonSimpleEmailServiceClientBuilder.standard()
          // Replace US_WEST_2 with the AWS Region you're using for
          // Amazon SES.
            .withRegion(Regions.US_WEST_2).build();
      SendEmailRequest request = new SendEmailRequest()
          .withDestination(
              new Destination().withToAddresses(TO))
          .withMessage(new Message()
              .withBody(new Body()
                  .withHtml(new Content()
                      .withCharset("UTF-8").withData(HTMLBODY))
                  .withText(new Content()
                      .withCharset("UTF-8").withData(TEXTBODY)))
              .withSubject(new Content()
                  .withCharset("UTF-8").withData(SUBJECT)))
          .withSource(FROM)
          // Comment or remove the next line if you are not using a
          // configuration set
          .withConfigurationSetName(CONFIGSET);
      client.sendEmail(request);
      System.out.println("Email sent!");
    } catch (Exception ex) {
      System.out.println("The email was not sent. Error message: "
          + ex.getMessage());
    }
  }
}
```

5. En `AmazonSESSample.java`, reemplace lo siguiente por sus propios valores:

> **Important**
>
> Las direcciones de correo electrónico distinguen entre mayúsculas y minúsculas. Asegúrese de que las direcciones sean exactamente las mismas que las que haya verificado.

- `SENDER@EXAMPLE.COM`: reemplácelo por su dirección de correo electrónico de remitente ("From"). Debe verificar esta dirección antes de ejecutar este programa. Para obtener más información, consulte Identidades verificadas en Amazon SES.
- `RECIPIENT@EXAMPLE.COM`: reemplácelo por su dirección de correo electrónico de destinatario ("To"). Si su cuenta está todavía en el entorno de pruebas, debe verificar esta dirección antes de utilizarla. Para obtener más información, consulte Solicitar acceso a la producción (salir del entorno de pruebas de Amazon SES).
- (Opcional) **`us-west-2`**: si desea utilizar Amazon SES en una región distinta a la de EE. UU. Oeste (Oregón), reemplácela por la región que desee utilizar. Para ver una lista de las regiones donde Amazon SES está disponible, consulte Amazon Simple Email Service (Amazon SES) en la Referencia general de AWS.

6. Guarde `AmazonSESSample.java`.
7. Para crear el proyecto, elija Project y, a continuación, elija Build Project.

> **Note**
>
> Si esta opción está deshabilitada, la creación automática podría estar habilitada; en tal caso, omita este paso.

8. Para iniciar el programa y enviar el correo electrónico, elija Run y, a continuación, vuelva a elegir Run.
9. Revise la salida del panel de consola en Eclipse. Si el correo electrónico se ha enviado correctamente, la consola muestra "`Email sent!`". De lo contrario, muestra un mensaje de error.
10. Si el correo electrónico se ha enviado correctamente, inicie sesión en el cliente de correo electrónico de la dirección del destinatario. Ahí podrá ver el mensaje que ha enviado.

PHP

En este tema, se muestra cómo utilizar AWS SDK for PHP para enviar un correo electrónico a través de Amazon SES.

Antes de empezar, lleva a cabo las tareas siguientes:

- Instale PHP: PHP está disponible en http://php.net/downloads.php. Este tutorial requiere PHP versión 5.5 o posterior. Después de instalar PHP, agregue la ruta a PHP en sus variables de entorno para que pueda ejecutar PHP desde cualquier símbolo del sistema. El código de este tutorial se ha probado con PHP 7.2.7.
- Instale la AWS SDK for PHP versión 3: para ver las instrucciones de descarga e instalación, consulte la AWS SDK for PHP documentación. El código de este tutorial se ha probado utilizando la versión 3.64.13 del SDK.

Para enviar un correo electrónico a través de Amazon SES utilizando el AWS SDK for PHP

1. En un editor de texto, cree un archivo con el nombre `amazon-ses-sample.php`. Pegue el siguiente código:

```
<?php

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

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

// Create an SesClient. Change the value of the region parameter if you're
// using an AWS Region other than US West (Oregon). Change the value of the
// profile parameter if you want to use a profile in your credentials file
// other than the default.
$SesClient = new SesClient([
    'profile' => 'default',
    'version' => '2010-12-01',
    'region'  => 'us-west-2'
]);

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

```
$sender_email = 'sender@example.com';

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

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

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

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

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

2. En `amazon-ses-sample.php`, reemplace lo siguiente por sus propios valores:

   - **`path_to_sdk_inclusion`**—Sustitúyala por la ruta requerida para incluirla AWS SDK for PHP en el programa. Para obtener más información, consulte la Documentación de AWS SDK for PHP.
   - **`sender@example.com`**: reemplace esta dirección por una dirección de email que haya verificado con Amazon SES. Para obtener más información, consulte Identidades verificadas. Las direcciones de email en Amazon SES distinguen entre mayúsculas y minúsculas. Asegúrese de que la dirección que introduce sea exactamente la misma que la que haya verificado.
   - **`recipient1@example.com`**, **`recipient2@example.com`**: sustitúyalos por la direcciones de los destinatarios. Si su cuenta está todavía en el entorno de pruebas, las direcciones de los destinatarios también se deben verificar. Para obtener más información, consulte Solicitar acceso a la producción (salir del entorno de pruebas de Amazon SES). Asegúrese de que la dirección que introduce sea exactamente la misma que la que haya verificado.
   - (Opcional) **`ConfigSet`**: si desea utilizar un conjunto de configuración al enviar este correo electrónico, sustituya este valor por el nombre del conjunto de configuración. Para obtener más información acerca de los conjuntos de configuración, consulte Uso de conjuntos de configuración en Amazon SES.
   - (Opcional) **`us-west-2`**: si desea utilizar Amazon SES en una región distinta a la de EE. UU. Oeste (Oregón), reemplácela por la región que desee utilizar. Para ver una lista de las regiones donde Amazon SES está disponible, consulte Amazon Simple Email Service (Amazon SES) en la Referencia general de AWS.

3. Guarde `amazon-ses-sample.php`.
4. Para ejecutar el programa, abra un símbolo del sistema en el directorio en que se encuentra `amazon-ses-sample.php` y, a continuación, escriba el comando siguiente:

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

5. Revise la salida. Si el correo electrónico se ha enviado correctamente, la consola muestra "`Email sent!`". De lo contrario, muestra un mensaje de error.

> **Note**
>
> Si detecta un error "cURL error 60: SSL certificate problem" (Error 60 de cURL: problema con el certificado SSL) al ejecutar el programa, descargue el último paquete de CA, tal como se describe en la documentación del AWS SDK for PHP. A continuación, en `amazon-ses-sample.php`, añada las siguientes líneas a la matriz `SesClient::factory`, reemplace `path_of_certs` por la ruta al paquete de CA que ha descargado y vuelva a ejecutar el programa.
>
> ```
> 'http' => [
>    'verify' => 'path_of_certs\ca-bundle.crt'
> ]
> ```

6. Inicie sesión en el cliente de correo electrónico de la dirección del destinatario. Ahí podrá ver el mensaje que ha enviado.

Ruby

En este tema, se muestra cómo utilizar AWS SDK for Ruby para enviar un correo electrónico a través de Amazon SES.

Antes de empezar, lleva a cabo las tareas siguientes:

- Instale Ruby: Ruby está disponible en https://www.ruby-lang.org/en/downloads/. El código de este tutorial se ha probado con Ruby 1.9.3. Después de instalar Ruby, añada la ruta a Ruby a sus variables de entorno para que pueda ejecutar Ruby desde cualquier símbolo del sistema.
- Instale el AWS SDK for Ruby —Para ver las instrucciones de descarga e instalación, consulte Instalación del AWS SDK for Ruby en la Guía para AWS SDK for Ruby desarrolladores. El

código de muestra de este tutorial se ha probado utilizando la versión 2.9.36 del AWS SDK for Ruby.

- Cree un archivo de credenciales compartidas: para que el código de muestra de esta sección funcione correctamente, debe crear un archivo de credenciales compartidas. Para obtener más información, consulte Crear un archivo de credenciales compartido para usarlo al enviar correos electrónicos a través de Amazon SES mediante un AWS SDK.

Para enviar un correo electrónico a través de Amazon SES utilizando el AWS SDK for Ruby

1. En un editor de texto, cree un archivo con el nombre `amazon-ses-sample.rb`. Pegue el código siguiente en el archivo:

```
require 'aws-sdk'

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

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

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

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

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

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

# The email body for recipients with non-HTML email clients.
```

```
textbody = "This email was sent with Amazon SES using the AWS SDK for Ruby."

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

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

# Try to send the email.
begin

  # Provide the contents of the email.
  resp = ses.send_email({
    destination: {
      to_addresses: [
        recipient,
      ],
    },
    message: {
      body: {
        html: {
          charset: encoding,
          data: htmlbody,
        },
        text: {
          charset: encoding,
          data: textbody,
        },
      },
      subject: {
        charset: encoding,
        data: subject,
      },
    },
  source: sender,
  # Comment or remove the following line if you are not using
  # a configuration set
  configuration_set_name: configsetname,
  })
  puts "Email sent!"

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

```
end
```

2. En `amazon-ses-sample.rb`, reemplace lo siguiente por sus propios valores:

   - **`sender@example.com`**: reemplace esta dirección por una dirección de email que haya verificado con Amazon SES. Para obtener más información, consulte Identidades verificadas. Las direcciones de email en Amazon SES distinguen entre mayúsculas y minúsculas. Asegúrese de que la dirección que introduce sea exactamente la misma que la que haya verificado.
   - **`recipient@example.com`**: reemplace esta dirección por la dirección del destinatario. Si su cuenta está todavía en el entorno de pruebas, debe verificar esta dirección antes de utilizarla. Para obtener más información, consulte Solicitar acceso a la producción (salir del entorno de pruebas de Amazon SES). Asegúrese de que la dirección que introduce sea exactamente la misma que la que haya verificado.
   - (Opcional) **`us-west-2`**: si desea utilizar Amazon SES en una región distinta a la de EE. UU. Oeste (Oregón), reemplácela por la región que desee utilizar. Para ver una lista de las regiones donde Amazon SES está disponible, consulte Amazon Simple Email Service (Amazon SES) en la Referencia general de AWS.
3. Guarde `amazon-ses-sample.rb`.
4. Para ejecutar el programa, abra un símbolo del sistema en el directorio en que se encuentra `amazon-ses-sample.rb` y, a continuación, escriba ruby amazon-ses-sample.rb.
5. Revise la salida. Si el correo electrónico se ha enviado correctamente, la consola muestra "`Email sent!`". De lo contrario, muestra un mensaje de error.
6. Inicie sesión en el cliente de correo electrónico de la dirección del destinatario. Encontrará el mensaje que ha enviado.

Python

En este tema, se muestra cómo utilizar AWS SDK for Python (Boto) para enviar un correo electrónico a través de Amazon SES.

Antes de empezar, lleva a cabo las tareas siguientes:

- Verifique su dirección de correo electrónico con Amazon SES: para poder enviar correo electrónico con Amazon SES, debe verificar que es propietario de la dirección de correo electrónico del remitente. Si su cuenta aún está en el entorno de pruebas de Amazon

SES, también tiene que verificar la dirección de correo electrónico del destinatario. Le recomendamos que utilice la consola de Amazon SES para verificar las direcciones de correo electrónico. Para obtener más información, consulte Creación de una identidad de dirección de correo electrónico.

- Obtenga sus AWS credenciales: necesita un identificador de clave de AWS acceso y una clave de acceso AWS secreta para acceder a Amazon SES mediante un SDK. Puede encontrar sus credenciales utilizando la página Security Credentials de la AWS Management Console. Para obtener más información acerca de las credenciales, consulte Tipos de credenciales de Amazon SES.
- Instale Python: Python está disponible en https://www.python.org/downloads/. El código de este tutorial se ha probado utilizando Python 2.7.6 y Python 3.6.1. Después de instalar Python, añada la ruta a Python a sus variables de entorno para que pueda ejecutar Python desde cualquier símbolo del sistema.
- Instale el AWS SDK for Python (Boto): para ver las instrucciones de descarga e instalación, consulte la AWS SDK for Python (Boto) documentación. El código de muestra de este tutorial se ha probado con la versión 1.4.4 del SDK para Python.

Para enviar un correo electrónico a través de Amazon SES con el SDK para Python.

1. En un editor de texto, cree un archivo con el nombre `amazon-ses-sample.py`. Pegue el código siguiente en el archivo:

```
import boto3
from botocore.exceptions import ClientError

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

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

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

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

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

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

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

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

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

# Try to send the email.
try:
    #Provide the contents of the email.
    response = client.send_email(
        Destination={
            'ToAddresses': [
                RECIPIENT,
            ],
        },
        Message={
            'Body': {
                'Html': {
```

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

2. En `amazon-ses-sample.py`, reemplace lo siguiente por sus propios valores:

   - **`sender@example.com`**: reemplace esta dirección por una dirección de email que haya verificado con Amazon SES. Para obtener más información, consulte Identidades verificadas. Las direcciones de correo electrónico en Amazon SES distinguen entre mayúsculas y minúsculas. Asegúrese de que la dirección que introduce sea exactamente la misma que la que haya verificado.
   - **`recipient@example.com`**: reemplace esta dirección por la dirección del destinatario. Si su cuenta está todavía en el entorno de pruebas, debe verificar esta dirección antes de utilizarla. Para obtener más información, consulte Solicitar acceso a la producción (salir del entorno de pruebas de Amazon SES). Asegúrese de que la dirección que introduce sea exactamente la misma que la que haya verificado.
   - (Opcional) **`us-west-2`**: si desea utilizar Amazon SES en una región distinta a la de EE. UU. Oeste (Oregón), reemplácela por la región que desee utilizar. Para ver una lista de las regiones donde Amazon SES está disponible, consulte Amazon Simple Email Service (Amazon SES) en la Referencia general de AWS.

3. Guarde `amazon-ses-sample.py`.
4. Para ejecutar el programa, abra un símbolo del sistema en el directorio en que se encuentra `amazon-ses-sample.py` y, a continuación, escriba python amazon-ses-sample.py.
5. Revise la salida. Si el correo electrónico se ha enviado correctamente, la consola muestra "`Email sent!`". De lo contrario, muestra un mensaje de error.
6. Inicie sesión en el cliente de correo electrónico de la dirección del destinatario. Ahí podrá ver el mensaje que ha enviado.

Crear un archivo de credenciales compartido para usarlo al enviar correos electrónicos a través de Amazon SES mediante un AWS SDK

El siguiente procedimiento muestra cómo crear un archivo de credenciales compartidas en su directorio de inicio. Para que el código de muestra de SDK funcione correctamente, debe crear este archivo.

1. En un editor de texto, cree un nuevo archivo. En el archivo, pegue el código siguiente:

```
[default]
aws_access_key_id = YOUR_AWS_ACCESS_KEY_ID
aws_secret_access_key = YOUR_AWS_SECRET_ACCESS_KEY
```

2. En el archivo de texto que acaba de crear, `YOUR_AWS_ACCESS_KEY` sustitúyalo por su ID de clave de AWS acceso único y `YOUR_AWS_SECRET_ACCESS_KEY` sustitúyalo por su clave de acceso AWS secreta única.
3. Guarde el archivo. En la siguiente tabla se muestra la ubicación correcta y el nombre de archivo de su sistema operativo.

Si utiliza...	Guarde el archivo como...
Windows	`C:\Users\<yourUserName>\.aws\credentials`
Linux, macOS o Unix	`~/.aws/credentials`

> **Important**
>
> No incluya una extensión de archivo cuando guarde el archivo de credenciales.

Codificaciones de contenido compatibles con Amazon SES

Se proporciona lo siguiente como referencia.

Amazon SES admite las siguientes codificaciones de código:

- `deflate`
- `gzip`
- `identity`

Amazon SES también admite el formato de encabezado Accept-Encoding, según la especificación 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 y los protocolos de seguridad

En este tema, se describen los protocolos de seguridad que puede utilizar al conectarse a Amazon SES, así como cuando Amazon SES entrega un correo electrónico a un receptor.

Remitente de correo electrónico para Amazon SES

El protocolo de seguridad que se utiliza para conectarse a Amazon SES depende de si se utiliza la API de Amazon SES o la interfaz de SMTP de Amazon SES, tal y como se describe a continuación.

HTTPS

Si utiliza la API de Amazon SES (directamente o mediante un AWS SDK), TLS cifra todas las comunicaciones a través del punto de enlace HTTPS de Amazon SES. El punto de conexión HTTPS de Amazon SES admite TLS 1.2 y TLS 1.3.

Interfaz de SMTP

Si obtiene acceso a Amazon SES a través de la interfaz de SMTP, deberá cifrar la conexión mediante Transport Layer Security (TLS). Tenga en cuenta que TLS se denomina en ocasiones con el nombre de su protocolo predecesor, capa de conexión segura (SSL).

Amazon SES admite dos mecanismos para establecer la conexión cifrada por TLS: STARTTLS y TLS Wrapper.

- STARTTLS: STARTTLS es un medio para actualizar una conexión sin cifrar a una conexión cifrada. Existen versiones de STARTTLS para diversos protocolos; la versión de SMTP se define en RFC 3207. Para las conexiones STARTTLS, Amazon SES admite TLS 1.2 y TLS 1.3.
- TLS Wrapper: TLS Wrapper (también conocido como SMTPS o protocolo Handshake) es un medio de iniciar una conexión cifrada sin establecer primero una conexión sin cifrar. Con TLS Wrapper, el punto de enlace de SMTP de Amazon SES no realiza la negociación de TLS: es responsabilidad del cliente conectarse al punto de enlace mediante TLS y seguir utilizando TLS para toda la conversación. TLS Wrapper es un protocolo más antiguo, pero muchos clientes siguen siendo compatibles. Para las conexiones TLS Wrapper, Amazon SES admite TLS 1.2 y TLS 1.3.

Para obtener información acerca de cómo conectarse a la interfaz de SMTP de Amazon SES mediante estos métodos, consulte Conexión a un punto de enlace de SMTP de Amazon SES.

Amazon SES al receptor

SES admite TLS 1.2 para las conexiones TLS. Para obtener más información, consulte Seguridad de la infraestructura en SES.

De forma predeterminada, Amazon SES utiliza TLS de forma oportuna. Esto significa que Amazon SES siempre intenta realizar una conexión segura al servidor de recepción de correo electrónico. Si Amazon SES no puede establecer una conexión segura, envía el mensaje sin cifrar.

Puede cambiar este comportamiento utilizando conjuntos de configuración. Utilice la operación de la API de PutConfigurationSetDeliveryopciones para establecer la `TlsPolicy` propiedad de una configuración establecida en. `Require` Puede utilizar la AWS CLI para realizar este cambio.

Para configurar Amazon SES para exigir conexiones TLS para un conjunto de configuración

- En la línea de comandos, escriba el comando siguiente.

  ```
  aws sesv2 put-configuration-set-delivery-options --configuration-set-
  name MyConfigurationSet --tls-policy REQUIRE
  ```

  En el ejemplo anterior, sustituya *MyConfigurationSet* por el nombre del conjunto de configuraciones.

  Cuando envía un correo electrónico a través de este conjunto de configuración, Amazon SES solo envía el mensaje al servidor de correo electrónico receptor si puede establecer una conexión segura. Amazon SES eliminará el mensaje si no puede realizar una conexión segura con el servidor de correo electrónico receptor.

nd-to-end Cifrado electrónico

Puede utilizar Amazon SES para enviar mensajes que se cifran mediante S/MIME o PGP. El remitente cifra los mensajes que utilizan estos protocolos. Solo los destinatarios que tengan las claves privadas necesarias para descifrar los mensajes pueden verlos.

Amazon SES admite los siguientes tipos MIME, que se pueden utilizar para enviar correo electrónico cifrado S/MIME:

- `application/pkcs7-mime`
- `application/pkcs7-signature`
- `application/x-pkcs7-mime`
- `application/x-pkcs7-signature`

Amazon SES también admite los siguientes tipos MIME, que se pueden utilizar para enviar correo electrónico cifrado PGP:

- `application/pgp-encrypted`

- `application/pgp-keys`
- `application/pgp-signature`

Campos de encabezado de Amazon SES

Amazon SES puede aceptar todos los encabezados de correo electrónico que siguen el formato descrito en RFC 822.

Los siguientes campos no pueden aparecer más de una vez en la sección de encabezado de un mensaje:

- `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`

Consideraciones

- El campo `acceptLanguage` no es estándar. Si es posible, debe utilizar el encabezado `Accept-Language` en su lugar.
- Si especifica un encabezado `Date`, Amazon SES lo anula con una marca temporal que se corresponde con la fecha y la hora de la zona horaria UTC cuando Amazon SES aceptó el mensaje.
- Si proporciona un encabezado `Message-ID`, Amazon SES anula el encabezado con su propio valor.
- Si especifica un encabezado `Return-Path`, Amazon SES envía notificaciones de rebotes y reclamos a la dirección especificada. Sin embargo, el mensaje que reciben los destinatarios contiene un valor diferente para el encabezado `Return-Path`.
- Si utiliza la `SendEmail` operación Amazon SES API v2 con contenido simple o con plantillas, o utiliza la `SendBulkEmail` operación, no podrá establecer un contenido de encabezado personalizado para los encabezados establecidos por SES; por lo tanto, los siguientes encabezados no están permitidos como encabezados personalizados:
  - `BCC`, `CC`, `Content-Disposition`, `Content-Type`, `Date`, `From`, `Message-ID`, `MIME-Version`, `Reply-To`, `Return-Path`, `Subject`, `To`

Tipos de adjuntos no compatibles con Amazon SES

Puede enviar mensajes con archivos adjuntos a través de Amazon SES utilizando el estándar Multipurpose Internet Mail Extensions (MIME). Amazon SES acepta todos los tipos de archivos adjuntos excepto archivos adjuntos con las extensiones de archivo de la siguiente lista.

.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

Algunos ISP tienen limitaciones adicionales (tales como restricciones en relación con los archivos adjuntos archivados), por lo que le recomendamos que pruebe el envío de correo electrónico a través de los principales ISP antes de enviar su correo electrónico de producción.

Recepción de correo electrónico con Amazon SES

Además de utilizar Amazon SES para administrar el envío de correo electrónico, también puede configurar SES para que reciba correo electrónico en nombre de uno o varios de sus dominios. Como receptor de correo electrónico, SES gestiona las operaciones de recepción de correo subyacentes, tales como la comunicación con otros servidores de correo, el análisis de spam y virus, el bloqueo de correo de fuentes que no sean de confianza (direcciones en las listas de bloqueo de Spamhaus o SES) y la aceptación de correo para los destinatarios de su dominio.

La extensión del procesamiento en el correo electrónico recibido viene determinada por las instrucciones personalizadas que especifique. Estas instrucciones se presentan de dos formas:

- Las reglas de recepción (control basado en destinatarios) proporcionan la granularidad más fina de control sobre el correo electrónico entrante. Las reglas de recepción pueden realizar un procesamiento avanzado, como entregar el correo entrante a un bucket de Amazon S3, publicarlo en un tema de Amazon SNS, enviarlo a Amazon WorkMail o enviar automáticamente mensajes de rebote cuando los mensajes se dirigen a direcciones de correo electrónico específicas, etc.
- Los filtros de direcciones IP (control basado en direcciones IP) proporcionan un amplio nivel de control y son fáciles de configurar. Estos filtros de direcciones IP permiten bloquear o permitir explícitamente todos los mensajes de direcciones IP o rangos de direcciones IP específicos.

Para comenzar el aprendizaje acerca de la recepción de correo electrónico, su configuración y la implementación mediante reglas de recepción o filtros de direcciones IP, primero revise Conceptos y casos de uso de recepción de correo electrónico para obtener información general de cómo funciona y las diferentes formas en que puede usarlo. A continuación, Configuración de la recepción de emails le guiará por los requisitos previos de configuración de recepción de correo electrónico. A continuación, Explicaciones de la consola acerca de la recepción de correo electrónico lo guiará por los asistentes utilizados para configurar reglas de recepción y filtros de direcciones IP.

> **Note**
>
> La recepción de correo electrónico solo se puede utilizar si la cuenta se encuentra en una Región de AWS donde SES admite la recepción de correo electrónico. Consulte Regiones de recepción de correo electrónico compatibles con SES.

Temas de esta sección:

- Conceptos y casos de uso de recepción de correo electrónico de Amazon SES
- Configuración de la recepción de correo electrónico de Amazon SES
- Explicaciones de la consola acerca de la recepción de correo electrónico de Amazon SES
- Visualización de métricas para la recepción de emails de Amazon SES

Conceptos y casos de uso de recepción de correo electrónico de Amazon SES

Al utilizar Amazon SES como receptor de correo electrónico, debe comunicar al servicio qué debe hacer con su correo electrónico. El método principal, las reglas de recepción, ofrece un control detallado acerca de la recepción de correo electrónico mediante el control basado en destinatarios para especificar un conjunto de acciones que se deben realizar en función del destinatario. El otro método, los filtros de direcciones IP, proporciona un amplio nivel de control basado en direcciones IP para bloquear o permitir el correo en función de la dirección IP o del intervalo de direcciones de origen.

Ambos métodos se describen en esta sección junto con información general de cómo Amazon SES procesa el correo electrónico recibido y casos de uso para ayudarle a considerar cómo desea recibir, filtrar y procesar el correo electrónico al configurar reglas y filtros.

Temas de esta sección:

- Control basado en destinatarios mediante reglas de recepción
- Control basado en IP mediante filtros de dirección IP
- Proceso de recepción de correo electrónico
- Casos de uso y restricciones para recibir correo electrónico de Amazon SES
- Autenticación de recepción de correo electrónico y análisis de malware

Control basado en destinatarios mediante reglas de recepción

La forma principal de controlar el correo entrante es especificar cómo se gestiona el correo mediante una lista ordenada de acciones para cualquiera de las identidades verificadas como dominios, subdominios o direcciones de correo electrónico. Tenga en cuenta que las direcciones de correo electrónico tienen que pertenecer a una de las identidades de dominio verificadas. Estas acciones se definen y ordenan en las reglas de recepción que crea en un conjunto de reglas.

Como opción, también puede agregar condiciones de destinatario como forma de especificar que las medidas solo se tomarán en caso de que el destinatario del correo entrante coincida con la identidad del destinatario especificada en la condición. Por ejemplo, si es propietario de example.com, puede especificar que el correo para user@example.com debe presentar rebotes y todo el resto de correo para example.com y sus subdominios deben entregarse.

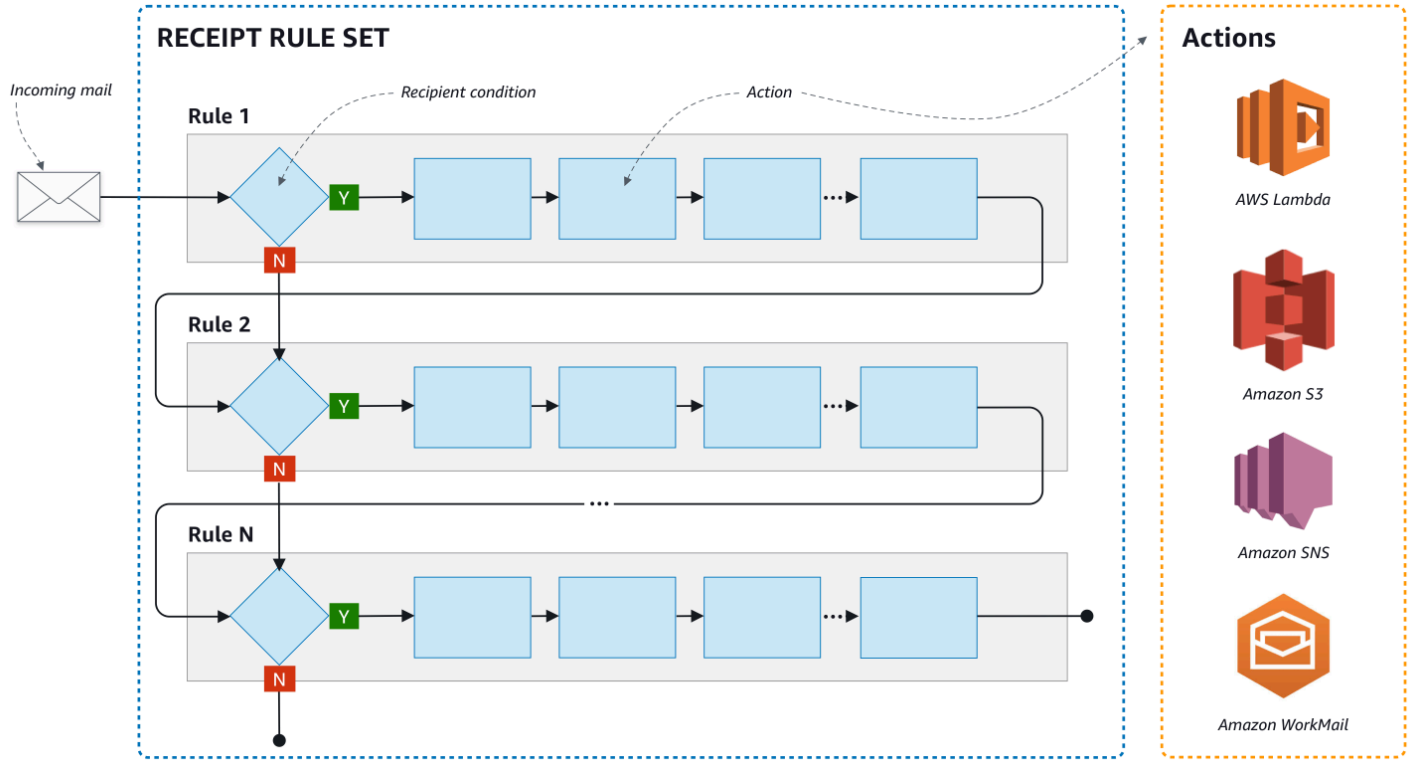
De lo contrario, si no agrega ninguna condición de destinatario, las acciones se aplicarán a todo: las direcciones de correo electrónico, los dominios y los subdominios que pertenezcan a sus dominios verificados. Las siguientes acciones están disponibles para aplicarlas a sus reglas de recepción:

- Acción Add header (Agregar encabezado): agrega un encabezado al correo electrónico recibido. Normalmente, utilice esta acción solo en combinación con otras acciones.
- Return bounce response action (Acción devolver respuesta de rebote): bloquea el correo electrónico devolviendo una respuesta de rebote al remitente y, opcionalmente, se lo notifica a través de Amazon SNS.
- Invoke AWS Lambda function action (Acción de invocar función de AWS Lambda): llama al código a través de una función de Lambda y, opcionalmente, se lo notifica a través de Amazon SNS.
- Acción Deliver to S3 bucket (Entregar a bucket de S3): entrega el correo a un bucket de Amazon S3 y, opcionalmente, se lo notifica a través de Amazon SNS.
- Acción Publish to Amazon SNS topic (Publicar en tema de Amazon SNS): publica el correo electrónico completo en un tema de Amazon SNS.

> **Note**
>
> La acción de SNS incluye una copia completa del contenido de correo electrónico en las notificaciones de Amazon SNS. Las demás opciones de notificación de Amazon SNS mencionadas aquí simplemente le notifican la entrega de correo electrónico; contienen información acerca del correo electrónico, no el propio contenido del correo electrónico.

- Acción Stop rule set (Detener conjunto de reglas): termina la evaluación del conjunto de reglas de recepción y, opcionalmente, se lo notifica a través de Amazon SNS.
- Acción Integrate with Amazon WorkMail (Integrar con Amazon WorkMail): gestiona el correo con Amazon WorkMail. Normalmente no utilizará esta acción directamente porque Amazon WorkMail se encarga de la configuración.

Las reglas de recepción se agrupan conjuntamente en conjuntos de reglas. Si no tiene ningún conjunto de reglas, tendrá que crear uno antes de comenzar a crear reglas de recepción. Puede definir varios conjuntos de reglas en su cuenta de AWS, pero solo se activa uno a la vez. La figura siguiente muestra cómo las reglas de recepción, los conjuntos de reglas y las acciones ese relacionan entre sí.



Control basado en IP mediante filtros de dirección IP

Puede controlar su flujo de correo mediante la configuración de filtros de direcciones IP. Los filtros de direcciones IP son opcionales y le permiten especificar si desea aceptar o bloquear correo electrónico procedente de una dirección IP o de un intervalo de direcciones IP. Sus filtros de direcciones IP pueden incluir listas de bloqueo (direcciones IP desde las que desea bloquear correo entrante) y listas permitidas (direcciones IP desde la que desea aceptar correo electrónico siempre).

Los filtros de direcciones IP son útiles para bloquear spam. Amazon SES mantiene su propia lista de bloqueo de direcciones IP conocidas por enviar spam, incluidas las mostradas en Spamhaus. Sin embargo, puede elegir recibir correo de dichas direcciones IP agregándolas a su lista de direcciones permitidas. Dado que no hay registros que muestren qué direcciones IP se están bloqueando, el remitente que está bloqueado tendrá que informarle. También es una buena oportunidad para ayudar al remitente a determinar si su dirección IP está en una lista de bloqueo, como Spamhaus y recomendar que solicite que no se incluya en la lista. Hacerlo será beneficioso tanto para usted como

para el remitente, ya que no tendrá que mantener un filtro de direcciones IP para él y mejorará su capacidad de entrega de correo electrónico.

> **Note**
>
> - Independientemente de la configuración del filtro de dirección IP, Amazon EC2 bloqueará el tráfico saliente en el puerto 25 (envío de correo) a menos que se incluya en la lista de permitidos. Consulte este artículo de AWS re:Post para obtener más información.
> - Si solo desea recibir emails de una lista finita de direcciones IP conocidas, entonces configure una lista de bloques que contenga `0.0.0.0/0` y configure una lista permitida que contenga las direcciones IP de confianza. Esta configuración bloquea todas las direcciones IP de forma predeterminada y solo permite correo de las direcciones IP que especifique de forma explícita.

Proceso de recepción de correo electrónico

Cuando Amazon SES recibe un correo electrónico para su dominio, se producen los eventos siguientes:

1. Amazon SES primero examina la dirección IP del remitente. Amazon SES permite que el correo electrónico supere esta fase a menos que:
   - La dirección IP se encuentre en la lista de bloqueo.
   - La dirección IP se encuentre en la lista de bloqueo de Amazon SES y no esté en su lista de direcciones permitidas.
2. Amazon SES examina su conjunto de sus reglas activas para determinar si alguna de sus reglas de recepción contiene una condición de destinatario:
   - Si existe una condición de destinatario y coincide con cualquiera de los destinatarios del correo electrónico entrante, Amazon SES acepta el correo electrónico. De lo contrario, si no se detectan coincidencias Amazon SES bloquea el correo electrónico.
   - Si la regla de recepción no contiene ninguna condición de destinatario, Amazon SES acepta el correo; todas las acciones de la regla se aplicarán a todas las identidades verificadas de su propiedad.
3. Amazon SES autentica el correo electrónico y analiza su contenido en busca de spam y malware:

- La dirección IP del host remoto que entregó el correo electrónico a Amazon SES se comprueba con la política SPF especificada en el dominio de MAIL FROM utilizado durante la transacción SMTP.
- Se comprueban las firmas DKIM presentes en la sección de encabezado del correo electrónico.
- Si el análisis de contenido está habilitado, el contenido del correo electrónico se analiza en busca de spam y malware.
- Los resultados de autenticación de correo electrónico y análisis de contenido se ponen a su disposición durante la evaluación de las reglas de recepción.

Para obtener más información, consulte Autenticación de correo electrónico y detección de malware.

4. Para el correo electrónico que Amazon SES acepta, todas las reglas de recepción de su conjunto de reglas activo se aplican en el orden que ha definido; en cada regla de recepción, las acciones se ejecutan en el orden que ha definido.

Casos de uso y restricciones para recibir correo electrónico de Amazon SES

En esta sección se examinan algunas consideraciones generales y algunos casos de uso para la recepción de correo electrónico de Amazon SES. Presentadas en formato de pregunta y respuesta, son preguntas y hechos comunes para ayudar a determinar si sería beneficioso utilizar Amazon SES para recibir y administrar el correo electrónico en nombre de uno o varios de los dominios verificados de su propiedad.

Disponibilidad en las regiones

¿Amazon SES admite la recepción de correo electrónico en su región?

Amazon SES solo admite la recepción de correo electrónico en determinadas regiones de AWS. Para obtener una lista completa de las regiones en las que se admite la recepción de correo electrónico, consulte Puntos de conexión y cuotas de Amazon Simple Email Service en la Referencia general de AWS.

Clientes de correo electrónico basados en POP o IMAP

¿Se puede usar Microsoft Outlook para recibir correo electrónico entrante?

Amazon SES no incluye servidores POP ni IMAP para recibir correo electrónico entrante. Esto significa que no puede utilizar un cliente de correo electrónico como Microsoft Outlook para recibir correo electrónico entrante. Si desea una solución que pueda enviar y recibir correo electrónico mediante un cliente de correo electrónico, considere la posibilidad de utilizar Amazon WorkMail.

Uso de otros servicios de AWS

¿Ha configurado los permisos adecuados?

Si desea que su correo se entregue en un bucket de S3, se publique en un tema de Amazon SNS que no sea de su propiedad, desencadene una función de Lambda o utilice una clave administrada por el cliente, tiene que conceder permiso a Amazon SES para acceder a dichos recursos. Para conceder acceso a Amazon SES, debe crear políticas de recursos desde las consolas o las API para dichos servicios de AWS. Para obtener más información, consulte Otorgar permiso.

Contenido de correo electrónico

¿Cómo desea que Amazon SES transfiera el contenido del correo electrónico?

Amazon SES puede proporcionarle el contenido del correo electrónico de dos formas: puede almacenar el correo electrónico en un bucket de S3 que especifique o bien enviarle una notificación de Amazon SNS que contenga una copia del correo electrónico. Amazon SES entrega el correo electrónico sin procesar y sin modificar en formato Multipurpose Internet Mail Extensions (MIME). Para obtener más información acerca del formato MIME, consulte RFC 2045.

Cómo de grandes son los emails que va a recibir?

Si almacena el correo electrónico en un bucket de S3, el tamaño de correo electrónico máximo (incluidos los encabezados) es de 40 MB. Si recibe el correo electrónico mediante notificaciones de Amazon SNS, el tamaño máximo del correo electrónico (incluidos los encabezados) es de 150 KB.

Cómo desea activar el procesamiento del email?

Una vez que se entregue el email, querrá procesarlo con su propio código. Por ejemplo, su aplicación podría convertir el email cifrado en base 64 a un formato que se pueda mostrar y, a continuación, hacer que esté disponible para un usuario final a través de un cliente de email. Hay una serie de formas en las que puede empezar el proceso:

- Si los correos electrónicos se entregan a Amazon S3, su aplicación puede escuchar las notificaciones de Amazon SNS generadas por las acciones de S3, extraer el ID de mensaje del

correo electrónico de las notificaciones y, a continuación, utilizar el ID de mensaje para recuperar el correo electrónico de Amazon S3.

De forma alternativa, puede incorporar el procesamiento de correo electrónico en las reglas de recepción si escribe una función de Lambda. En este caso, la regla de recepción debe escribir primero el correo electrónico en Amazon S3 y, a continuación, desencadenar la función de Lambda. Las acciones de Lambda se pueden ejecutar de forma sincrónica o asincrónica desde las reglas de recepción, en función de si la función Lambda necesita devolver un resultado que impacte en la forma en que se ejecutan otras acciones. Le recomendamos que use la ejecución asincrónica, a menos que la sincrónica sea absolutamente necesaria en su caso de uso. Para obtener más información sobre AWS Lambda, consulte la AWS LambdaGuía para desarrolladores de .

- Si los correos electrónicos se entregan a través de una notificación de Amazon SNS mediante la acción de SNS, la aplicación puede escuchar las notificaciones de Amazon SNS y, a continuación, extraer los mensajes de correo electrónico de las notificaciones.

¿Desea que los emails se cifren?

Amazon SES se integra con AWS Key Management Service (AWS KMS) para cifrar opcionalmente el correo electrónico que escribe en el bucket de S3. Amazon SES utiliza el cifrado del lado del cliente para cifrar el correo electrónico antes de escribirlo en Amazon S3. Esto significa que deberá descifrar el contenido en su lado después de recuperar el correo electrónico de Amazon S3. El AWS SDK for Java y AWS SDK for Ruby proporcionan un cliente que puede encargarse de gestionar el descifrado. Amazon SES solo puede cifrar los correos electrónicos si elige que estos se entreguen en un bucket de S3.

Correo no deseado

¿En qué punto del proceso de recepción de emails desea bloquear los correos electrónicos no deseados?

Cuando un remitente intenta enviar un email a un destinatario, el servidor de email del remitente intercambia una secuencia de comandos con el servidor del destinatario. Esta secuencia se denomina conversación SMTP.

Puede bloquear el correo electrónico entrante en dos puntos en el proceso de recepción de correo electrónico: durante la conversación SMTP y después de esta. Se utilizan filtros de direcciones IP

para bloquear mensajes durante la conversación SMTP y reglas de recepción para bloquear correos electrónicos después de la conversación SMTP.

Puede utilizar filtros de direcciones IP para bloquear correo electrónico procedente de determinadas direcciones IP. El beneficio de utilizar filtros de direcciones IP para bloquear correo no deseado es que no le cobraremos los mensajes que se bloquean durante la conversación SMTP. La desventaja de utilizar filtros de direcciones IP es que bloquean correo electrónico desde las direcciones IP que especifique sin realizar ningún análisis sobre el contenido real de los mensajes. Para obtener más información sobre los filtros de direcciones IP, consulte Explicación de la consola de creación de filtros de direcciones IP.

Puede utilizar reglas de recepción para enviar una notificación de rebote al remitente de un email en función de la dirección (o dominio, o subdominio) a la que se envió el mensaje. El beneficio de utilizar reglas de recepción es que puede llevar a cabo un análisis adicional en los mensajes entrantes antes de enviar una notificación de rebote al remitente. Por ejemplo, puede utilizar AWS Lambda para enviar las notificaciones de rebote solo cuando los mensajes no superen la autenticación DKIM o se identifiquen como spam. La desventaja de utilizar las reglas de recepción es que, dado que las reglas de recepción se procesan después de la conversación SMTP, se facturan todos los mensajes que reciba. También es posible que se le cobre si utiliza Lambda para analizar el contenido de los mensajes entrantes. Para obtener más información sobre las reglas de recepción, consulte Explicación de la consola sobre la creación de reglas de recepción. Para obtener más información acerca de cómo utilizar Lambda para analizar correo electrónico entrante, consulte Ejemplos de funciones de Lambda.

Flujos de correo

¿Cómo desea separar el flujo de emails?

Es probable que su dominio reciba distintas clases de emails. Por ejemplo, parte de los emails de su dominio, tal como un email a user@example.com, podría estar destinado a una bandeja de correo personal. Otros mensajes, tal como un email a unsubscribe@example.com, podrían ir dirigidos a sistemas automáticos. Puede utilizar reglas de recepción para separar el correo entrante a fin de que se pueda procesar de forma distinta. Para obtener información sobre cómo configurar las reglas de recepción, consulte Creación de reglas de recepción.

Autenticación de recepción de correo electrónico y análisis de malware

Amazon SES autentica cada correo electrónico recibido y, opcionalmente, escanea el contenido del correo electrónico en busca de spam y malware. SES no realiza ninguna acción sobre el correo

electrónico recibido en función de los resultados de la autenticación de correo electrónico o del análisis de contenido; sin embargo, los resultados de estas operaciones se le proporcionan como atributos que puede utilizar en las acciones de las reglas de recepción de SES, como notificaciones de Amazon SNS o como encabezados de un mensaje entregado a Amazon S3.

Autenticación de correo electrónico

Amazon SES autentica cada correo electrónico recibido mediante SPF, DKIM y DMARC. Los resultados de cada mecanismo de autenticación se proporcionan en las notificaciones de Amazon SNS que SES envía como parte de la evaluación de las reglas en el conjunto de reglas de recepción activas. Además, si eligió recibir una copia del correo electrónico en Amazon S3, el resultado de la autenticación de correo electrónico se recoge en el encabezado `Authentication-Results` que SES agrega a la sección de encabezado del correo electrónico:

```
Authentication-Results: example.com;
spf=pass (spfCheck: 10.0.0.1 is permitted by domain of example.com) client-ip=10.0.0.1;
 envelope-from=example@example.com; helo=10.0.0.1;
dkim=pass header.i=example.com;
dkim=permerror header.i=some-example.com;
dmarc=pass header.from=example@example.com;
```

El encabezado `Authentication-Results` se describe en RFC 8601

Análisis del contenido del correo electrónico en busca de detección de spam y malware

Amazon SES analiza el contenido del correo electrónico recibido en busca de malware en función del valor del atributo de ScanEnabled(API) o Análisis de spam y virus (Análisis de spam y virus) (consola) de la regla de recepción que coincide con el correo electrónico. De forma predeterminada, SES escanea el contenido del correo electrónico recibido en busca de malware. Para desactivar el análisis de contenido de correos electrónicos recibidos que coinciden con una regla de recepción específica, debe establecer el indicador ScanEnabled de la regla de recepción en falso si usa la API, o desmarque la casilla Spam and virus scanning (Análisis de spam y virus) si usa la consola. Si la regla de recepción que coincide con un correo electrónico está habilitada para escanear, el resultado del análisis de contenido se proporciona en las notificaciones de Amazon SNS que SES envía como parte de la evaluación de las reglas en el conjunto de reglas de recepción activas. Además, si eligió recibir una copia del correo electrónico en Amazon S3, el resultado del escaneo del contenido se recoge en los encabezados `X-SES-Spam-Verdict` y `X-SES-Virus-Verdict` que SES agrega a la sección de encabezados del correo electrónico.

```
X-SES-Spam-Verdict: PASS
```

```
X-SES-Virus-Verdict: FAIL
```

Los valores posibles para los encabezados anteriores se clasifican como:

- spam
- virus

Ahora que ya dispone de información sobre los conceptos de recepción de correo electrónico, cómo funciona y sus casos de uso, puede dirigirse a Configuración de la recepción de emails para comenzar.

Configuración de la recepción de correo electrónico de Amazon SES

En esta sección se describen los requisitos previos necesarios para comenzar a configurar Amazon SES para recibir su correo. Es importante que haya leído Conceptos y casos de uso de recepción de correo electrónico para comprender los conceptos sobre el funcionamiento de Amazon SES y para plantearse la forma en que desea recibir, filtrar y procesar su correo electrónico.

Antes de configurar la recepción de correo electrónico mediante la creación de un conjunto de reglas, reglas de recepción y filtros de direcciones IP, primero debe completar los siguientes requisitos previos de configuración:

- Verifique su dominio con Amazon SES. Para ello, publique los registros DNS para demostrar que es el propietario.
- Permita que Amazon SES reciba correo electrónico para su dominio mediante la publicación de un registro MX.
- Conceda permiso a Amazon SES para acceder a otros recursos de AWS a fin de poder ejecutar acciones de reglas de recepción.

Al crear y verificar una identidad de dominio, publica registros en la configuración de DNS para completar el proceso de verificación, pero esto por sí solo no es suficiente para usar la recepción de correo electrónico. Específicamente para la recepción de correo electrónico, también es necesario publicar un registro MX para especificar un dominio de correo electrónico personalizado. Este registro se utiliza en la configuración de DNS de su dominio para permitir que SES reciba correo electrónico para su dominio. Es necesario conceder permisos porque las acciones que elija en las

reglas de recepción no funcionarán a menos que Amazon SES tenga permiso para utilizar el servicio de AWS respectivo requerido para esas acciones.

Estos tres requisitos previos necesarios para utilizar la recepción de correo electrónico se explican en los temas siguientes:

- Verificación de su dominio para recepción de correo electrónico de Amazon SES
- Publicación de un registro MX para la recepción de correo electrónico de Amazon SES
- Otorgar permisos a Amazon SES para recepción de correo electrónico

Verificación de su dominio para recepción de correo electrónico de Amazon SES

Al igual que con cualquier dominio que desee utilizar para enviar o recibir correo electrónico a través de Amazon SES, primero debe demostrar que es de su propiedad. El procedimiento de verificación incluye iniciar la verificación del dominio con SES y luego publicar los registros DNS, ya sea CNAME o TXT, a su proveedor de DNS de acuerdo con el método de verificación que utilice.

Desde la consola, puede verificar sus dominios con Easy DKIM o Bring Your Own DKIM (BYODKIM) y copiar con facilidad sus registros DNS para publicarlos en su proveedor de DNS, procedimiento que se explica en Creación de una identidad de dominio. Si lo desea, puede utilizar las API `VerifyDomainDkim` o `VerifyDomainIdentity` de SES.

Para confirmar que su dominio o dirección de correo electrónico esté verificado, puede consultar su estado en la tabla Verified identities (Identidades verificadas) de la consola de SES o utilizar las API `GetIdentityVerificationAttributes` o `GetEmailIdentity` de SES.

Publicación de un registro MX para la recepción de correo electrónico de Amazon SES

Un registro de intercambio de correo (registro MX#) es una configuración que especifica los servidores de correo que pueden aceptar emails enviados al dominio.

Para que Amazon SES administre su correo electrónico entrante, debe agregar un registro MX a la configuración de DNS del dominio. El registro MX que crea hace referencia al punto de enlace que recibe correo electrónico para la región de AWS en la que se utiliza Amazon SES. Por ejemplo, el punto de enlace de la región EE. UU. Oeste (Oregón) es inbound-smtp.us-west-2.amazonaws.com.

Para obtener una lista completa de puntos de enlace, consulte Regiones y puntos de enlace de Amazon SES.

> **Note**
>
> Los puntos de enlace que reciben correo electrónico en Amazon SES no son servidores de correo electrónico IMAP ni POP3. No se pueden utilizar estas direcciones URL como servidores de emails entrante en clientes de email.
> Si desea una solución que pueda enviar y recibir correo electrónico mediante un cliente de correo electrónico, considere la posibilidad de utilizar Amazon WorkMail.

El siguiente procedimiento incluye pasos generales para crear un registro MX. Los procedimientos específicos para crear un registro MX dependen del proveedor de DNS o de alojamiento. Consulte la documentación del proveedor para obtener más información sobre cómo añadir un registro MX a la configuración DNS de su dominio.

> **Note**
>
> Para completar el siguiente procedimiento, tiene que poder modificar los registros de DNS del dominio. Si no puede obtener acceso a los registros de DNS de su dominio o no está familiarizado con este proceso, póngase en contacto con su administrador del sistema para obtener ayuda.

Para añadir un registro MX a la configuración de DNS de su dominio.

1. Inicie sesión en la consola de administración del proveedor de DNS.
2. Cree un nuevo registro MX.
3. Para el Name (Nombre) del registro MX, especifique el dominio. Por ejemplo, si desea que Amazon SES administre el correo electrónico que se envía al dominio example.com, ingrese lo siguiente:

   ```
   example.com
   ```

> **Note**
>
> Algunos proveedores de DNS hacen referencia al campo Name (Nombre) como Host, Domain (Dominio) o Mail Domain (Dominio de correo).

4. En Type (Tipo), seleccione MX.

> **Note**
>
> Algunos proveedores de DNS se refieren al campo Type (Tipo) como Record Type (Tipo de registro) o un nombre similar.

5. En Value (Valor), introduzca lo siguiente:

```
10 inbound-smtp.region.amazonaws.com
```

En el ejemplo anterior, reemplace *region* por la dirección del punto de conexión que recibe correo electrónico para la región de AWS que utiliza con Amazon SES. Por ejemplo, si está utilizando la región EE. UU. Este (Norte de Virginia), reemplace el valor de *region* por `us-east-1`. Para obtener una lista completa de puntos de enlace, consulte Regiones y puntos de enlace de Amazon SES.

> **Note**
>
> Las consolas de administración de algunos proveedores de DNS incluyen campos independientes para el registro Value (Valor) y el registro Priority (Prioridad). Si es el caso para su proveedor de DNS, introduzca `10` para el valor Priority (Prioridad) e introduzca la siguiente URL de punto de enlace de correo entrante para Value (Valor).

Instrucciones para crear registros MX para diversos proveedores

Los procedimientos para crear un registro MX para su dominio dependen del proveedor de DNS utilizado. Esta sección incluye enlaces a la documentación de diversos varios proveedores de DNS habituales. Este listado de proveedores no es exhaustivo. Si su proveedor no aparece en la lista siguiente, probablemente podrá seguir utilizándolo con Amazon SES. La inclusión en esta lista no supone ningún tipo de respaldo o recomendación de los productos o servicios de ninguna empresa.

Nombre del proveedor de alojamiento/DNS	Enlace a la documentación
Amazon Route 53	Creación de registros con la consola de Amazon Route 53
GoDaddy	Add an MX record (enlace externo)
DreamHost	How do I change my MX records? (enlace externo)
Cloudflare	Configurar registros de correo electrónico (enlace externo)
HostGator	Changing MX records - Windows (enlace externo)
Namecheap	How can I set up MX records required for mail service? (enlace externo)
Names.co.uk	Changing your domain's DNS settings (enlace externo)
Wix	Adding or Updating MX Records in Your Wix Account (enlace externo)

Otorgar permisos a Amazon SES para recepción de correo electrónico

Algunas de las tareas que puede realizar cuando recibe correo electrónico en Amazon SES, como enviar correo electrónico a un bucket de Amazon Simple Storage Service (Amazon S3) o llamar a una función de AWS Lambda, requieren permisos especiales. Esta sección incluye políticas de ejemplo para diferentes casos de uso comunes.

Temas de esta sección:

- Otorgue permiso a Amazon SES para escribir en un bucket de S3
- Otorgar permiso a Amazon SES para utilizar la clave de AWS KMS
- Conceder permiso a Amazon SES para invocar una función de AWS Lambda

- Conceder permiso a Amazon SES para la publicación en un tema de Amazon SNS que pertenece a una cuenta de AWS diferente

Otorgue permiso a Amazon SES para escribir en un bucket de S3

Cuando se aplica la siguiente política a un bucket de S3, se otorga permiso a Amazon SES para escribir en dicho bucket. Para obtener más información acerca de la creación de reglas de recepción que transfieren el correo electrónico entrante a Amazon S3, consulte Entregar a la acción del bucket de S3.

Para obtener más información acerca de la asociación de políticas a buckets de S3, consulte Uso de políticas de bucket y políticas de usuario en la Guía del usuario de Amazon Simple Storage Service.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AllowSESPuts",
      "Effect":"Allow",
      "Principal":{
        "Service":"ses.amazonaws.com"
      },
      "Action":"s3:PutObject",
      "Resource":"arn:aws:s3:::myBucket/*",
      "Condition":{
        "StringEquals":{
          "AWS:SourceAccount":"111122223333",
          "AWS:SourceArn": "arn:aws:ses:region:111122223333:receipt-rule-
set/rule_set_name:receipt-rule/receipt_rule_name"
        }
      }
    }
  ]
}
```

En la política de ejemplo anterior, realice los siguientes cambios:

- Reemplace *myBucket* por el nombre del bucket de S3 en el que desea escribir.
- Reemplace *region* por la región de AWS en la que creó la regla de recepción.
- Reemplace *111122223333* por su ID de cuenta de AWS.

- Reemplace *rule_set_name* con el nombre del conjunto de reglas que contiene la regla de recepción que posee la acción de bucket de entrega a Amazon S3.
- Reemplace *nombre_rule_receptor* con el nombre de la regla de recepción que contiene la acción de bucket de entrega a Amazon S3.

Otorgar permiso a Amazon SES para utilizar la clave de AWS KMS

Para que Amazon SES cifre los correos electrónicos, debe tener permiso para utilizar la clave de AWS KMS especificada al configurar la regla de recepción. Puede utilizar la clave de KMS predeterminada (aws/ses) de su cuenta o bien una clave administrada por el cliente que cree. Si utiliza la clave de KMS predeterminada, no tiene que realizar ningún paso adicional para conceder permiso a Amazon SES para que la utilice. Si utiliza una clave administrada por el cliente, debe otorgar permiso a Amazon SES para utilizarla mediante la adición de una instrucción a la política de la clave.

Utilice la siguiente instrucción de política como la política de clave para permitir que Amazon SES utilice su clave administrada por el cliente cuando reciba emails en su dominio.

```
{
  "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"
        }
      }
}
```

En la política de ejemplo anterior, realice los siguientes cambios:

- Reemplace *region* por la región de AWS en la que creó la regla de recepción.

- Reemplace *111122223333* por su ID de cuenta de AWS.
- Reemplace *rule_set_name* con el nombre del conjunto de reglas que contiene la regla de recepción que ha asociado con la recepción de emails.
- Reemplace *nombre_rule_receptor* con el nombre de la regla de recepción que ha asociado con la recepción de emails.

Si utiliza AWS KMS para enviar mensajes cifrados a un bucket de S3 con el cifrado del lado del servidor habilitado, a continuación, debe agregar la acción de política, `"kms:Decrypt"`. Con el ejemplo anterior, agregar esta acción a la política aparecerá de la siguiente manera:

```
{
  "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"
        }
      }
}
```

Para obtener más información sobre cómo adjuntar políticas a claves de AWS KMS, consulte Uso de políticas de claves en AWS KMS en laGuía para desarrolladores de AWS Key Management Service.

Conceder permiso a Amazon SES para invocar una función de AWS Lambda

Para permitir que Amazon SES llame a una función de AWS Lambda, puede elegir la función cuando cree una regla de recepción en la consola de Amazon SES. Al hacerlo, Amazon SES agrega automáticamente los permisos necesarios a la función.

También puede utilizar la operación `AddPermission` en la API de AWS Lambda para adjuntar una política a una función. La siguiente llamada a la API de `AddPermission` concede permiso a Amazon SES para invocar su función de Lambda. Para obtener más información sobre cómo adjuntar políticas a funciones de Lambda, consulte Permisos de AWS Lambda en la Guía para desarrolladores de 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"
}
```

En la política de ejemplo anterior, realice los siguientes cambios:

- Reemplace *region* por la región de AWS en la que creó la regla de recepción.
- Reemplace *111122223333* por su ID de cuenta de AWS.
- Reemplace *rule_set_name* por el nombre del conjunto de reglas que contiene la regla de recepción en la que creó la función de Lambda.
- Reemplace *receipt_rule_name* por el nombre de la regla de recepción que contiene la función de Lambda.

Conceder permiso a Amazon SES para la publicación en un tema de Amazon SNS que pertenece a una cuenta de AWS diferente

Si desea publicar notificaciones sobre un tema en una cuenta de AWS diferente, deberá adjuntar una política al tema de Amazon SNS. El tema de SNS debe estar en la misma región que el conjunto de reglas de dominio y de recepción.

La siguiente política concede permiso a Amazon SES para la publicación en un tema de Amazon SNS en una cuenta de AWSdiferente.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
```

```
      "Principal":{
        "Service":"ses.amazonaws.com"
      },
      "Action":"SNS:Publish",
      "Resource":"arn:aws:sns:topic_region:sns_topic_account_id:topic_name",
      "Condition":{
        "StringEquals":{
          "AWS:SourceAccount":"aws_account_id",
          "AWS:SourceArn": "arn:aws:ses:receipt_region:aws_account_id:receipt-rule-
set/rule_set_name:receipt-rule/receipt_rule_name"
        }
      }
    }
  ]
}
```

En la política de ejemplo anterior, realice los siguientes cambios:

- Reemplace *topic_region* por la Región de AWS en el que se creó el tema de Amazon SNS.
- Reemplace *sns_topic_account_id* por el ID de la cuenta de AWS propietaria del tema de Amazon SNS.
- Reemplace *topic_name* por el nombre del tema de Amazon SNS en el que desea publicar notificaciones.
- Reemplace *aws_account_id* por el ID de la cuenta de AWS configurada para recibir correo electrónico.
- Reemplace *receipt-region* por la Región de AWS en la que creó la regla de recepción.
- Reemplace *rule_set_name* por el nombre del conjunto de reglas que contiene la regla de recepción en la que creó la acción de publicación en el tema de Amazon SNS.
- Reemplace *receipt_rule_name* por el nombre de la regla de recepción que contiene la acción de publicación en el tema de Amazon SNS.

Si el tema de Amazon SNS utiliza AWS KMS para el cifrado del lado del servidor, tendrá que agregar permisos a la política de claves de AWS KMS. Puede añadir permisos asociando la siguiente política a la política de claves de AWS KMS:

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "AllowSESToUseKMSKey",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

Explicaciones de la consola acerca de la recepción de correo electrónico de Amazon SES

En esta sección se describen los asistentes de la consola de recepción de correo electrónico que se utilizan para configurar reglas de recepción y filtros de direcciones IP para administrar la recepción de su correo electrónico. Antes de usar los asistentes de la consola, es importante que haya leído tanto Conceptos y casos de uso de recepción de correo electrónico, para entender los conceptos del funcionamiento de la recepción de correo electrónico, como Configuración de la recepción de emails, para asegurarse de haber completado los requisitos previos de configuración.

Los asistentes de consola para configurar reglas de recepción y filtros de direcciones IP se explican en:

- Explicación de la consola sobre la creación de reglas de recepción
- Explicación de la consola de creación de filtros de direcciones IP

Explicación de la consola sobre la creación de reglas de recepción

Esta sección le guiará a través de la creación y definición de reglas de recepción mediante la consola de Amazon SES. Los puntos clave para entender cómo funcionan las reglas de recepción son los siguientes:

- Los conjuntos de reglas contienen un conjunto ordenado de reglas de recepción; las reglas de recepción contienen un conjunto ordenado de acciones.

- Las reglas de recepción indican a Amazon SES cómo gestionar el correo entrante mediante la ejecución de una lista ordenada de acciones que especifique.
- Esta lista ordenada de acciones puede depender de forma opcional de la primera coincidencia de una condición de destinatario; si no se especifica, las acciones se aplicarán a todas las identidades que pertenezcan a sus dominios verificados.
- Las reglas de recepción se crean y definen en un contenedor denominado “conjunto de reglas”; aunque puede crear varios conjuntos de reglas, solo uno puede estar activo a la vez.
- Las reglas de recepción del juego de reglas activo se ejecutan en el orden que especifique.
- Antes de crear las reglas de recepción, primero debe crear un conjunto de reglas que las contenga.

De forma opcional, puede utilizar la API de `CreateReceiptRuleSet` para crear un conjunto de reglas de recepción vacío, tal como se describe en la Referencia de la API de Amazon Simple Email Service. A continuación, puede utilizar la consola de Amazon SES o la API de `CreateReceiptRule` para agregarle reglas de recepción.

Antes de continuar con la explicación, asegúrese de haber cumplido todos los requisitos previos necesarios para utilizar la recepción de correo electrónico basada en destinatarios. También

Requisitos previos

Se deben cumplir los siguientes requisitos previos para continuar con la configuración del control de correo electrónico basado en destinatarios mediante las reglas de recepción:

1. Asegúrese de que el punto de conexión esté en una Región de AWS en la que Amazon SES sea compatible con la recepción de correo electrónico. Consulte los puntos de conexión de recepción de correo electrónico compatibles con SES.
2. En primer lugar, debe crear y verificar una identidad de dominio en Amazon SES.
3. A continuación, debe especificar qué servidores de correo pueden aceptar correo para su dominio mediante la publicación de un registro MX en la configuración de DNS de su dominio. (El registro MX debe hacer referencia al punto de enlace de Amazon SES que recibe correo electrónico para la región de AWS en la que se utiliza Amazon SES).
4. Por último, debe conceder permiso a Amazon SES para acceder a otros recursos de AWS a fin de poder ejecutar acciones de reglas de recepción.

Creación de conjuntos de reglas y reglas de recepción

Esta explicación comienza con la creación de un conjunto de reglas que contenga las reglas y progresa hacia el asistente para crear reglas para crear, definir y ordenar las reglas de recepción. El asistente contiene cuatro pantallas para definir la configuración de reglas, agregar condiciones de destinatarios, agregar acciones y revisar toda la configuración.

Para crear un conjunto de reglas y reglas de recepción con la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Email Receiving (Recepción de correo electrónico).

   > **Note**
   >
   > La recepción de correo electrónico no estará visible en el panel de navegación izquierdo de la consola de SES si la cuenta se encuentra en una Región de AWS en la que SES no admite la recepción de correo electrónico. Consulte el primer elemento que se muestra en the section called “Requisitos previos”.

3. En la pestaña Receipt rule sets (Conjuntos de reglas de recepción) del panel de Email receiving (Recepción de correo electrónico), seleccione Create rule set (Crear conjunto de reglas).
4. Ingrese un nombre único para el conjunto de reglas y elija Create rule set (Crear conjunto de reglas).
5. Elija Create rule (Crear regla) y se abrirá el asistente para crear reglas.
6. En la página Define rule settings (Definir la configuración de reglas), en Receipt rule details (Detalles de reglas de recepción), ingrese un nombre en Rule name (Nombre de la regla).
7. En Status (Estado), solo desmarque la casilla Enabled (Habilitado) si no desea que Amazon SES ejecute esta regla después de la creación; de lo contrario, deje esta opción marcada.
8. (Opcional) En Security and protection options (Opciones de seguridad y protección), en Transport Layer Security (TLS) (Seguridad de la capa de transporte [TLS]), seleccione Required (Obligatorio) si desea que Amazon SES rechace los mensajes entrantes que no se envíen a través de una conexión segura.
9. (Opcional) En Spam and virus scanning (Análisis de spam y virus), seleccione Enabled (Habilitado) si desea que Amazon SES analice los mensajes entrantes en busca de spam y virus.

10. Para continuar en el paso siguiente, elija Next (Siguiente).
11. (Opcional) En la página Add recipient conditions (Agregar condiciones de destinatario), utilice el procedimiento siguiente para especificar una o más condiciones de destinatario. Puede tener un máximo de 100 condiciones de destinatario por regla de recepción.

    a. En Recipient conditions (Condiciones del destinatario), elijaAdd new recipient condition (Agregar nueva condición de destinatario) para especificar la dirección de correo electrónico o el dominio de recepción al que quiere aplicar la regla de recepción. En la siguiente tabla se utiliza la dirección user@example.com para mostrar cómo especificar condiciones de destinatario.

Si desea…	Especifique los siguientes destinatarios...	Notas
Haga coincidir una dirección de email específica.	user@example.com	Haga coincidir también variaciones de la dirección que contengan etiquetas (como usuario+123@example.com y usuario+xyz@example.com). No obstante, si especifica una dirección que contenga una etiqueta, solo se hace coincidir dicha dirección específica.
Haga coincidir todas las direcciones dentro de un dominio, pero no aquellas dentro de sus subdominios.	example.com	
Haga coincidir todas las direcciones dentro de un subdominio específico, pero no aquellas dentro del dominio principal.	subdomain.example.com	

Si desea…	Especifique los siguientes destinatarios...	Notas
Haga coincidir todas las direcciones dentro de todos los subdominios, pero no aquellas dentro del dominio principal.	.example.com	Tenga en cuenta el punto (.) antes del nombre de dominio.
Haga coincidir todas las direcciones dentro de un dominio y todas las direcciones dentro de todos sus subdominios.	example.com .example.com	Crear dos destinatarios independientes: uno con el nombre de dominio y otro con un punto seguido del nombre de dominio.
Haga coincidir todos los destinatarios en todos los dominios verificados	[Ninguno]	Deje en blanco el campo de destinatario.

> **Important**
>
> Si varias cuentas de Amazon SES reciben correo electrónico en un dominio común (por ejemplo, si varios equipos de la misma empresa tienen cuentas de Amazon SES independientes), Amazon SES procesa todas las reglas de recepción coincidentes de forma simultánea para cada una de las cuentas. Este comportamiento puede hacer que una cuenta rebote el email, mientras que otra lo acepte.
>
> Le recomendamos que se coordine con otros equipos de la organización que utilicen Amazon SES para garantizar que cada cuenta utilice reglas de recepción únicas y que estas reglas no se solapen. En estas situaciones, es mejor configurar las reglas de recepción para utilizar solo direcciones de email o subdominios que sean únicos del grupo o equipo.

b. Repita este paso para cada condición de destinatario que desee agregar. Cuando haya terminado de agregar condiciones de destinatario, elija Next (Siguiente).

12. En la página Add actions (Agregar acciones), utilice el siguiente procedimiento para agregar una o más acciones a la regla de recepción.

    a. Abra el menú Add new action (Agregar nueva acción) y, a continuación, elija uno de los tipos de acciones siguientes:

    - Add header (Agregar encabezado): esta acción agrega un encabezado personalizado al correo electrónico recibido.
    - Devolver respuesta de rebote: esta acción rechaza el correo electrónico recibido y devuelve una respuesta de rebote al remitente.
    - Invocación de una función Lambda: esta acción llama a su código a través de una función de AWS Lambda.
    - Entregar al bucket de S3: esta acción almacena el correo electrónico recibido en un bucket de Amazon Simple Storage Service (S3).
    - Publicación en un tema de Amazon SNS: esta acción publica el correo electrónico completo en un tema de Amazon Simple Notification Service (SNS).
    - Detención del conjunto de reglas: esta acción termina la evaluación del conjunto de reglas de recepción.
    - Integración con Amazon WorkMail: esta acción se integra con Amazon WorkMail.

    Para obtener más información acerca de cada una de estas acciones, consulte Opciones de las acciones.

    b. Repita este paso para cada acción que desee definir. Si tiene varias acciones definidas, puede reordenarlas utilizando las flechas arriba/abajo en los contenedores de acciones. Elija Next (Siguiente) para abrir la página Review (Revisar).

13. En la página Review (Revisar), revise la configuración y las acciones de la regla. Si necesita realizar cambios, elija la opción Edit (Editar) o utilice la sección de navegación del lado izquierdo de la página para ir directamente al paso con el contenido que desea editar. Si lo desea, puede realizar cambios en el orden de las acciones enumeradas en la tabla Actions (Acciones) de la página Review (Revisar) mediante las flechas arriba/abajo de la columna Reorder (Reordenar).
14. Cuando esté listo para continuar, elija Create rule (Crear regla).
15. En la página de confirmación del conjunto de reglas, elija Set as active (Establecer como activo) si desea aplicar el conjunto de reglas inmediatamente.

Modificaciones de reglas tras la creación

Después de crear un conjunto de reglas, puede editar tanto el conjunto de reglas como las reglas de recepción que contiene. No solo se pueden editar, sino que también existe la opción de duplicar el conjunto de reglas o sus reglas para poder crear otras nuevas rápidamente. En la lista siguiente se muestran las modificaciones disponibles para el conjunto de reglas y las reglas de recepción:

- El conjunto de reglas se muestra con su nombre, estado y fecha de creación. Las opciones de modificación para el conjunto de reglas son:
  - El botón de alternancia Set as active/inactive (Establecer como activo/inactivo) alternará la configuración de estado.
  - El botón Duplicate (Duplicar) copiará el conjunto de reglas. Se le pedirá que proporcione un nombre único.
  - El botón Delete (Eliminar) eliminará el conjunto de reglas. Se le pedirá que confirme esta acción irreversible.
- Las reglas de recepción se enumeran con su nombre, estado, seguridad y orden. Las opciones de modificación para las reglas de recepción son:
  - Flechas arriba/abajo para reordenar la ejecución de reglas en el conjunto de reglas.
  - El botón Duplicate (Duplicar) creará una copia de la regla seleccionada. Se le pedirá que proporcione un nombre único.
  - El botón Edit (Editar) abrirá la regla seleccionada para que se pueda editar cualquiera de sus parámetros, como la configuración de reglas, las condiciones de destinatario y las acciones.
  - El botón Delete (Eliminar) eliminará la regla seleccionada. Se le pedirá que confirme esta acción irreversible.
  - El botón Create rule (Crear regla) le permitirá crear y agregar una nueva regla al conjunto de reglas actual.

Opciones de las acciones

Cada regla de recepción para recibir correo electrónico de Amazon SES contiene una lista ordenada de acciones. En esta sección, se describen las opciones específicas para cada tipo de acción.

Los tipos de acción son los siguientes:

- Acción Add header (Agregar encabezado)
- Acción de devolución de respuesta de rebote

- Acción de invocación de una función de Lambda
- Entregar a la acción del bucket de S3
- Acción de publicación en un tema de Amazon SNS
- Acción de detención del conjunto de reglas
- Acción de integración con Amazon WorkMail

Acción Add header (Agregar encabezado)

La acción Add Header (Agregar encabezado) agrega un encabezado personalizado al email recibido. Normalmente, utilice esta acción solo en combinación con otra acción. Esta acción tiene las siguientes opciones.

- Header name: nombre del encabezado que se va a agregar. Debe tener entre 1 y 50 caracteres, incluidos y consta únicamente de caracteres alfanuméricos (a-z, A-Z, 0-9) y guiones.
- Header value: valor del encabezado que se va a agregar. Debe tener menos de 2 048 caracteres y no debe contener caracteres de línea nueva ("\r" o "\n").

Acción de devolución de respuesta de rebote

La acción Bounce (Rebotar) rechaza el correo electrónico. Para ello, devuelve una respuesta de rebote al remitente y, opcionalmente, se lo notifica a usted a través de Amazon SNS. Esta acción tiene las siguientes opciones.

- SMTP Reply Code: el código de respuesta SMTP, tal como define RFC 5321.
- SMTP Status Code: el código de estado mejorado SMTP, tal como define RFC 3463.
- Message (Mensaje): texto en lenguaje natural para incluir en el email de rebote.
- Reply Sender: dirección de correo electrónico del remitente del correo electrónico rebotado. Es la dirección desde la que se enviará el email de rebote. Se debe verificar con Amazon SES.
- SNS Topic (Tema de SNS): nombre o ARN del tema de Amazon SNS para enviar una notificación opcional cuando se envía un email de rebote. Un ejemplo de un ARN de tema de Amazon SNS es: arn:aws:sns:us-east-1:123456789012:MyTopic. Para crear un tema de Amazon SNS al configurar la acción, puede elegir Create SNS Topic (Crear tema de SNS). Para obtener más información acerca de los temas de Amazon SNS, consulte la Guía para desarrolladores de Amazon Simple Notification Service.

> **Note**
>
> El tema de Amazon SNS que elija deberá estar en la misma región de AWS que el punto de conexión de Amazon SES que utilice para recibir correo electrónico.

Puede introducir sus propios valores para estos campos o bien puede elegir una plantilla que rellene los campos SMTP Reply Code, SMTP Status Code y Message con valores en función del motivo del rebote. Están disponibles las siguientes plantillas:

- Mailbox Does Not Exist: código de respuesta de SMTP = 550, código de estado SMTP = 5.1.1
- Message Too Large: código de respuesta de SMTP = 552, código de estado SMTP = 5.3.4
- Message Full: código de respuesta de SMTP = 552, código de estado SMTP = 5.2.2
- Message Content Rejected: código de respuesta de SMTP = 500, código de estado SMTP = 5.6.1
- Unknown Failure: código de respuesta de SMTP = 554, código de estado SMTP = 5.0.0
- Temporary Failure: código de respuesta de SMTP = 450, código de estado SMTP = 4.0.0

Para obtener códigos de rebote adicionales que podría utilizar introduciendo valores personalizados en los campos, consulte RFC 3463.

Acción de invocación de una función de Lambda

La acción de Lambda llama al código a través de una función de Lambda y, opcionalmente, se lo notifica a usted a través de Amazon SNS. Esta acción tiene las siguientes opciones y requisitos.

Opciones

- Lambda function (Función de Lambda): ARN de la función de Lambda. Un ejemplo de ARN de una función de Lambda es arn:aws:lambda:us-east-1:account-id:function:MyFunction.
- Invocation type (Tema de invocación): tipo de invocación de la función de Lambda. Un tipo de invocación de RequestResponse (Solicitud de respuesta) significa que la ejecución de la función da como resultado una respuesta inmediata. Un tipo de invocación de Event (Evento) significa que la función se invoca de forma asíncrona. Le recomendamos que utilice el tipo de invocación Event (Evento) a menos que su caso de uso requiera la ejecución sincrónica.

  Se produce un desfase de 30 segundos en las invocaciones RequestResponse.

Para obtener más información, consulte Invocar funciones de Lambda en la Guía para desarrolladores de AWS Lambda.

- SNS Topic (Tema de SNS): nombre o ARN del tema de Amazon SNS al que se debe enviar la notificación cuando se desencadena la función de Lambda especificada. Un ejemplo de un ARN de tema de Amazon SNS es: arn:aws:sns:us-east-1:123456789012:MyTopic. Para obtener instrucciones, consulte el tema Creación de un tema de Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.

Requisitos

- La función de Lambda que elija deberá estar en la misma región de AWS que el punto de conexión de Amazon SES que utilice para recibir correo electrónico.
- El tema de Amazon SNS que elija deberá estar en la misma región de AWS que el punto de conexión de Amazon SES que utilice para recibir correo electrónico.

Escritura de la función de Lambda

Para procesar el correo electrónico, la función de Lambda se puede invocar de manera asíncrona (es decir, utilizando el tipo de invocación `Event`). El objeto de evento transferido a su función de Lambda contendrá metadatos pertenecientes al evento de correo electrónico de entrada. También puede utilizar los metadatos para acceder al contenido del mensaje desde su bucket de Amazon S3.

Si desea controlar realmente el flujo de correo electrónico, debe invocar la función de Lambda de forma síncrona (es decir, utilizando el tipo de invocación `RequestResponse`) y la función de Lambda debe llamar al método `callback` con dos argumentos: el primer argumento es `null` y el segundo argumento es una propiedad `disposition` que se establece en `STOP_RULE`, `STOP_RULE_SET` o `CONTINUE`. Si el segundo argumento es `null` o no tiene una propiedad `disposition` válida, el flujo de correo continúa y se procesan acciones y reglas adicionales, que es lo mismo que con `CONTINUE`.

Por ejemplo, puede detener el conjunto de reglas de recepción escribiendo la siguiente línea al final del código de la función de Lambda:

```
callback( null, { "disposition" : "STOP_RULE_SET" });
```

Para obtener ejemplos de código de AWS Lambda, consulte Ejemplos de funciones de Lambda. Para ver ejemplos de casos de uso de alto nivel, consulte Ejemplos de casos de uso.

Formato de entrada

Amazon SES transfiere información a la función de Lambda en formato JSON. El objeto de nivel superior contiene una matriz `Records`, que se rellena con las propiedades `eventSource`, `eventVersion` y `ses`. El objeto `ses` contiene objetos `receipt` y `mail`, que tienen exactamente el mismo formato que en las notificaciones de Amazon SNS descritas en Contenido de las notificaciones.

Los datos que Amazon SES transmite a Lambda incluyen metadatos acerca del mensaje, así como varios encabezados de correo electrónico. Sin embargo, no contiene el cuerpo del mensaje.

A continuación, se ofrece una vista de alto nivel de la estructura de la entrada que Amazon SES proporciona a la función de Lambda.

```
{
   "Records": [
      {
        "eventSource": "aws:ses",
        "eventVersion": "1.0",
        "ses": {
           "receipt": {
               <same contents as SNS notification>
            },
           "mail": {
               <same contents as SNS notification>
           }
         }
      }
   ]
}
```

Return values

La función de Lambda puede controlar el flujo de correo electrónico devolviendo uno de los siguientes valores:

- `STOP_RULE`: no se procesarán acciones adicionales en la regla de recepción actual, pero se pueden procesar reglas de recepción adicionales.
- `STOP_RULE_SET`: no se procesarán acciones o reglas de recepción adicionales.
- `CONTINUE` o cualquier otro valor no válido: esto significa que se pueden procesar acciones y reglas de recepción adicionales.

En los siguientes temas se tratan ejemplos de eventos de correo electrónico entrante, ejemplos de casos de uso de alto nivel y ejemplos de código de AWS Lambda:

- Ejemplos de casos de uso
- Ejemplos de funciones de Lambda

Ejemplos de casos de uso

Los siguientes ejemplos describen algunas reglas que podría configurar para utilizar los resultados de la función de Lambda para controlar el flujo de correo electrónico. Para fines de demostración, muchos de estos ejemplos utilizan la acción de S3 como resultado.

Caso de uso 1: Rechazar spam en todos los dominios

Este ejemplo muestra una regla global que rechaza spam en todos sus dominios. Las reglas 2 y 3 se incluyen para mostrar que puede aplicar reglas específicas de dominio después de rechazar el spam en todos los dominios.

Regla 1

Lista de destinatarios: vacía. Esta regla, por tanto, se aplicará a todos los destinatarios en todos los dominios verificados.

Acciones

1. Acción Lambda (síncrona) que devuelve `STOP_RULE_SET` si el email es spam. De lo contrario, devuelve `CONTINUE`. Consulte el ejemplo de la función de Lambda para rechazar spam en Ejemplos de funciones de Lambda.

Regla 2

Lista de destinatarios: example1.com

Acciones

1. Cualquier acción.

Regla 3

Lista de destinatarios: example2.com

Acciones

1. Cualquier acción.

Caso de uso 2: Rebotar spam en todos los dominios

Este ejemplo muestra una regla global que rebota spam en todos sus dominios. Las reglas 2 y 3 se incluyen para mostrar que puede aplicar reglas específicas de dominio después de rebotar el spam en todos los dominios.

Regla 1

Lista de destinatarios: vacía. Esta regla, por tanto, se aplicará a todos los destinatarios en todos los dominios verificados.

Acciones

1. Acción Lambda (síncrona) que devuelve `CONTINUE` si el email es spam. De lo contrario, devuelve `STOP_RULE`.
2. Acción de rebote ("500 5.6.1. Message content rejected").
3. Acción Stop.

Regla 2

Lista de destinatarios: example1.com

Acciones

1. Cualquier acción

Regla 3

Lista de destinatarios: example2.com

Acciones

1. Cualquier acción

Caso de uso 3: Aplicar la regla más específica

Este ejemplo ilustra cómo puede utilizar la acción Stop (Detener) para impedir que varias reglas procesen los emails. En este ejemplo, dispone de una regla para una dirección específica y de otra para todas las direcciones de email del dominio. Al utilizar la acción Stop (Detener), los mensajes que coinciden con la regla de la dirección de emails específica no se procesan con la regla más genérica que se aplica al dominio.

Regla 1

Lista de destinatarios: user@example.com

Acciones

1. Acción Lambda (asíncrona)
2. Acción Stop.

Regla 2

Lista de destinatarios: example.com

Acciones

1. Cualquier acción.

Caso de uso 4: Registrar eventos de correo en CloudWatch

Este ejemplo muestra cómo mantener un registro de auditoría de todo el correo que pasa por el sistema antes de guardar el correo en Amazon SES.

Regla 1

Lista de destinatarios: example.com

Acciones

1. Acción de Lambda (asíncrona) que escribe el objeto de evento en un registro de CloudWatch. Las funciones de Lambda de muestra de Ejemplos de funciones de Lambda se registran en CloudWatch.
2. Acción S3.

Caso de uso 5: Rechazar correo que no supera DKIM

Este ejemplo muestra cómo puede guardar todo el correo electrónico entrante en un bucket de Amazon S3, pero solo enviar correo electrónico que vaya a una dirección de correo electrónico específica y supere DKIM, a su aplicación de correo electrónico automatizada.

Regla 1

Lista de destinatarios: example.com

Acciones

1. Acción S3.
2. Acción Lambda (síncrona) que devuelve `STOP_RULE_SET` si el mensaje no supera DKIM. De lo contrario, devuelve `CONTINUE`.

Regla 2

Lista de destinatarios: support@example.com

Acciones

1. Acción Lambda (asíncrona) que activa la aplicación automatizada.

Caso de uso 6: Filtrar correo en función de la línea de asunto

Este ejemplo ilustra cómo puede rechazar todo el email entrante de un dominio que contenga la palabra "descuento" en la línea de asunto y, a continuación, procesar los emails destinados a un sistema automatizado de forma unidireccional y procesar todo el email dirigido a todos los demás destinatarios del dominio de una forma diferente.

Regla 1

Lista de destinatarios: example.com

Acciones

1. Acción Lambda (síncrona) que devuelve `STOP_RULE_SET` si la línea de asunto contiene la palabra "descuento". De lo contrario, devuelve `CONTINUE`.

Regla 2

Lista de destinatarios: support@example.com

Acciones

1. Acción S3 con bucket 1.
2. Acción Lambda (asíncrona) que activa la aplicación automatizada.
3. Acción Stop.

Regla 3

Lista de destinatarios: example.com

Acciones

1. Acción S3 con bucket 2.
2. Acción Lambda (asíncrona) que procesa el email para el resto del dominio.

Ejemplos de funciones de Lambda

Este tema contiene ejemplos de funciones de Lambda que controlan el flujo de correo.

Ejemplo 1: Rechazar spam

Este ejemplo detiene el procesamiento de mensajes que tienen al menos un indicador de spam.

```
exports.handler = function(event, context, callback) {
    console.log('Spam filter');

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

    // Check if any spam check failed
    if (sesNotification.receipt.spfVerdict.status === 'FAIL'
            || sesNotification.receipt.dkimVerdict.status === 'FAIL'
            || sesNotification.receipt.spamVerdict.status === 'FAIL'
            || sesNotification.receipt.virusVerdict.status === 'FAIL') {
        console.log('Dropping spam');
        // Stop processing rule set, dropping message
        callback(null, {'disposition':'STOP_RULE_SET'});
    } else {
```

```
        callback(null, null);
    }
};
```

Ejemplo 2: Continuar si se encuentra un encabezado en particular

Este ejemplo continúa el procesamiento de la regla actual únicamente si el email contiene un valor de encabezado específico.

```
exports.handler = function(event, context, callback) {
    console.log('Header matcher');

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

    // Iterate over the headers
    for (var index in sesNotification.mail.headers) {
        var header = sesNotification.mail.headers[index];

        // Examine the header values
        if (header.name === 'X-Header' && header.value === 'X-Value') {
            console.log('Found header with value.');
            callback(null, null);
            return;
        }
    }

    // Stop processing the rule if the header value wasn't found
    callback(null, {'disposition':'STOP_RULE'});
};
```

Ejemplo 3: Recuperar correo electrónico de Amazon S3

Este ejemplo obtiene el correo electrónico sin procesar de Amazon S3 y lo procesa.

> **Note**
>
> En primer lugar, debe escribir el correo electrónico en Amazon S3 con una acción de S3.

```
var AWS = require('aws-sdk');
var s3 = new AWS.S3();
```

```
var bucketName = '<YOUR BUCKET GOES HERE>';

exports.handler = function(event, context, callback) {
    console.log('Process email');

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

    // Retrieve the email from your bucket
    s3.getObject({
            Bucket: bucketName,
            Key: sesNotification.mail.messageId
        }, function(err, data) {
            if (err) {
                console.log(err, err.stack);
                callback(err);
            } else {
                console.log("Raw email:\n" + data.Body);

                // Custom email processing goes here

                callback(null, null);
            }
        });
};
```

Ejemplo 4: Rebotar los mensajes que no superan la autenticación DMARC

Este ejemplo envía un mensaje de rebote si un email entrante no supera la autenticación DMARC.

> **Note**
>
> Cuando utilice este ejemplo, defina el valor de la variable de entorno `emailDomain` en su dominio de recepción de emails.

```
'use strict';

const AWS = require('aws-sdk');

// Assign the emailDomain environment variable to a constant.
```

```
const emailDomain = process.env.emailDomain;

exports.handler = (event, context, callback) => {
    console.log('Spam filter starting');

    const sesNotification = event.Records[0].ses;
    const messageId = sesNotification.mail.messageId;
    const receipt = sesNotification.receipt;

    console.log('Processing message:', messageId);

    // If DMARC verdict is FAIL and the sending domain's policy is REJECT
    // (p=reject), bounce the email.
    if (receipt.dmarcVerdict.status === 'FAIL'
        && receipt.dmarcPolicy.status === 'REJECT') {
        // The values that make up the body of the bounce message.
        const sendBounceParams = {
            BounceSender: `mailer-daemon@${emailDomain}`,
            OriginalMessageId: messageId,
            MessageDsn: {
                ReportingMta: `dns; ${emailDomain}`,
                ArrivalDate: new Date(),
                ExtensionFields: [],
            },
            // Include custom text explaining why the email was bounced.
            Explanation: "Unauthenticated email is not accepted due to the sending
 domain's DMARC policy.",
            BouncedRecipientInfoList: receipt.recipients.map((recipient) => ({
                Recipient: recipient,
                // Bounce with 550 5.6.1 Message content rejected
                BounceType: 'ContentRejected',
            })),
        };

        console.log('Bouncing message with parameters:');
        console.log(JSON.stringify(sendBounceParams, null, 2));
        // Try to send the bounce.
        new AWS.SES().sendBounce(sendBounceParams, (err, data) => {
            // If something goes wrong, log the issue.
            if (err) {
                console.log(`An error occurred while sending bounce for message:
 ${messageId}`, err);
                callback(err);
            // Otherwise, log the message ID for the bounce email.
```

```
            } else {
                console.log(`Bounce for message ${messageId} sent, bounce message ID:
 ${data.MessageId}`);
                // Stop processing additional receipt rules in the rule set.
                callback(null, {
                    disposition: 'stop_rule_set',
                });
            }
        });
    // If the DMARC verdict is anything else (PASS, QUARANTINE or GRAY), accept
    // the message and process remaining receipt rules in the rule set.
    } else {
        console.log('Accepting message:', messageId);
        callback();
    }
};
```

Entregar a la acción del bucket de S3

La acción S3 envía el correo electrónico a un bucket de Amazon S3 y, opcionalmente, se lo notifica a través de Amazon SNS. Esta acción tiene las siguientes opciones.

- S3 Bucket (Bucket de S3): nombre del bucket de Amazon S3 en el que se guardan los correos electrónicos recibidos. También puede crear un nuevo bucket de Amazon S3 cuando configura la acción al elegir Create S3 Bucket (Crear un bucket de S3). Amazon SES proporciona el correo electrónico sin procesar y sin modificar que normalmente está en formato Multipurpose Internet Mail Extensions (MIME). Para obtener más información acerca del formato MIME, consulte RFC 2045.

  > **Important**
  >
  > - Cuando guarda los correos electrónicos en un bucket de Simple Storage Service (Amazon S3), el tamaño máximo predeterminado del correo electrónico (incluidos los encabezados) es de 40 MB.
  > - SES no admite reglas de recepción que se carguen en los buckets de S3 habilitados con el bloqueo de objetos y configurados con un periodo de retención predeterminado.
  > - Si aplica el cifrado en su bucket de S3 mediante la especificación de su propia clave de KMS, asegúrese de utilizar el ARN completo de la clave de KMS, y no el alias de la clave. El uso del alias puede hacer que los datos se cifren con una clave de KMS que

pertenece al solicitante, y no al administrador del bucket. Consulte Uso del cifrado con operaciones entre cuentas.

- SES no admite buckets de S3 en regiones registradas como destino de los correos electrónicos entrantes.

- Object Key Prefix (Prefijo de clave de objeto): un prefijo de nombre de clave para utilizar dentro del bucket de Amazon S3. Los prefijos de nombre de clave permiten organizar el bucket de Amazon S3 en una estructura de carpetas. Por ejemplo, si utiliza Email (Correo electrónico) como Object Key Prefix, (Prefijo de clave de objeto) los correos electrónicos aparecerán en el bucket de Amazon S3 en una carpeta denominada Email.
- Clave de KMS (si selecciona “Encrypt Message” [Cifrar mensajes] en la consola de Amazon SES): la clave de AWS que Amazon SES debería utilizar para cifrar sus correos electrónicos antes de guardarlos en el bucket de Amazon S3. Puede utilizar la clave de KMS predeterminada o una clave administrada del cliente que usted creó en AWS KMS.

> **Note**
>
> La clave de KMS que elija deberá estar en la misma región de AWS que el punto de enlace de Amazon SES que utilice para recibir correo electrónico.

  - Para utilizar la clave de KMS predeterminada, elija aws/ses al configurar la regla de recepción en la consola de Amazon SES. Si utiliza la API de Amazon SES, puede especificar la clave de KMS predeterminada si proporciona un ARN con el formato `arn:aws:kms:REGION:AWSACCOUNTID:alias/aws/ses`. Por ejemplo, si su ID de cuenta de AWS es 123456789012 y desea utilizar la clave de KMS predeterminada en la región us-east-1, el ARN de la clave de KMS predeterminada sería `arn:aws:kms:us-east-1:123456789012:alias/aws/ses`. Si usa la clave de KMS predeterminada, no tiene que realizar ningún paso adicional para conceder permiso a Amazon SES para que utilice la clave.
  - Para utilizar una clave administrada personalizada que ha creado en AWS KMS, proporcione el ARN de la clave de KMS y asegúrese de agregar una instrucción a su política de claves para otorgar permiso a Amazon SES para utilizarla. Para obtener más información sobre la concesión de permisos, consulte Otorgar permisos a Amazon SES para recepción de correo electrónico.

Para obtener más información acerca del uso de AWS KMS con Amazon SES, consulte la Guía para desarrolladores de AWS Key Management Service. Si no especifica una clave de KMS en la consola o la API, Amazon SES no cifrará los correos electrónicos.

> **Important**
>
> Amazon SES cifra el email utilizando el cliente de cifrado de Amazon S3 antes de que el email se envíe a Amazon S3 para su almacenamiento. No se cifra con el cifrado del lado del servidor de Amazon S3. Esto significa que debe utilizar el cliente de cifrado de Amazon S3 para descifrar el correo electrónico después de recuperarlo de Amazon S3, ya que el servicio no tiene acceso para utilizar sus claves de AWS KMS para el descifrado. Este cliente de cifrado está disponible en el AWS SDK for Java y en el AWS SDK for Ruby. Para obtener más información, consulte la Guía del usuario de Amazon Simple Storage Service.

- SNS Topic (Tema de SNS): nombre o ARN del tema de Amazon SNS para notificar cuando se guarda un correo electrónico en el bucket de Amazon S3. Un ejemplo de un ARN de tema de Amazon SNS es: arn:aws:sns:us-east-1:123456789012:MyTopic. Para crear un tema de Amazon SNS al configurar la acción, puede elegir Create SNS Topic (Crear tema de SNS). Para obtener más información acerca de los temas de Amazon SNS, consulte la Guía para desarrolladores de Amazon Simple Notification Service.

  > **Note**
  >
  > El tema de Amazon SNS que elija deberá estar en la misma región de AWS que el punto de enlace de Amazon SES que utilice para recibir correo electrónico.

Acción de publicación en un tema de Amazon SNS

La acción de SNS publica el correo con una notificación de Amazon SNS. La notificación incluye todo el contenido del email. Esta acción tiene las siguientes opciones.

- SNS Topic (Tema de SNS): nombre o ARN del tema de Amazon SNS en el que se publican los correos electrónicos. Las notificaciones de Amazon SNS contendrán una copia del correo electrónico sin modificar y sin procesar, que normalmente está en formato Multipurpose Internet Mail Extensions (MIME). Para obtener más información acerca del formato MIME, consulte RFC 2045.

> **Important**
>
> Si decide recibir los correos electrónicos mediante notificaciones de Amazon SNS, el tamaño máximo del correo electrónico (incluidos los encabezados) es de 150 KB. Los emails de mayor tamaño rebotarán. Si prevé utilizar correos electrónicos de un tamaño mayor, guárdelos en un bucket de Amazon S3.

Un ejemplo de un ARN de tema de Amazon SNS es: arn:aws:sns:us-east-1:123456789012:MyTopic. Para crear un tema de Amazon SNS al configurar la acción puede elegir Create SNS Topic (Crear tema de SNS). Para obtener más información acerca de los temas de Amazon SNS, consulte la Guía para desarrolladores de Amazon Simple Notification Service.

> **Note**
>
> El tema de Amazon SNS que elija deberá estar en la misma región de AWS que el punto de enlace de Amazon SES que utilice para recibir correo electrónico.

- Encoding (Cifrado): cifrado que se va a utilizar para el correo electrónico en la notificación de Amazon SNS. UTF-8 es más fácil de utilizar, pero no conservará todos los caracteres especiales si un mensaje se ha cifrado con un formato de cifrado diferente. Base64 conserva todos los caracteres especiales. Para obtener información sobre UTF-8 y Base64, consulte RFC 3629 y RFC 4648, respectivamente.

Cuando se recibe un correo electrónico, Amazon SES ejecuta las reglas del conjunto de reglas de recepción activo. Puede configurar reglas de recepción para que se le envíen notificaciones mediante Amazon SNS. Las reglas de recepción pueden enviar dos tipos distintos de notificaciones:

- Notificaciones enviadas desde acciones de SNS: cuando se agrega una acción de SNS a una regla de recepción, esta envía información acerca del correo electrónico, así como su contenido. Si el mensaje tiene 150 KB o menos, este tipo de notificación también incluye el cuerpo MIME completo del correo electrónico.
- Notificaciones enviadas desde otros tipos de acciones: cuando agrega cualquier otro tipo de acción (incluidas las acciones Bounce, Lambda, Stop Rule Set o WorkMail) a una regla de recepción, es posible de especificar un tema de Amazon SNS. Si lo hace, recibirá notificaciones

cuando se realicen estas acciones. Estas notificaciones contienen información sobre el correo electrónico, pero no incluyen el contenido del correo electrónico.

En los temas siguientes se describe el contenido de estas notificaciones y se ofrece un ejemplo de cada tipo de notificación:

- Contenido de las notificaciones para recibir correo electrónico de Amazon SES
- Ejemplos de notificaciones para recepción de correo electrónico de Amazon SES

Contenido de las notificaciones para recibir correo electrónico de Amazon SES

Todas las notificaciones de recepción de correo electrónico se publican en temas de Amazon Simple Notification Service (Amazon SNS) en formato de notación de objetos JavaScript (JSON).

Para obtener ejemplos de notificaciones, consulte Ejemplos de notificaciones.

Contenido

- Objeto JSON de nivel superior
- Objeto receipt
  - Objeto action
  - Objeto dkimVerdict
  - Objeto dmarcVerdict
  - Objeto spamVerdict
  - Objeto spfVerdict
  - Objeto virusVerdict
- Objeto mail
  - Objeto commonHeaders

Objeto JSON de nivel superior

Los objetos JSON de nivel superior contienen los siguientes campos.

Nombre del campo	Descripción
`notificationType`	El tipo de notification. Para este tipo de notificación, el valor siempre es `Received`.

Nombre del campo	Descripción
`receipt`	Objeto que contiene información sobre la entrega de correo electrónico.
`mail`	Objeto que contiene información sobre el correo electrónico relacionado con la notificación.
`content`	Cadena que contiene el correo electrónico sin procesar y sin modificar que normalmente está en formato Multipurpose Internet Mail Extensions (MIME). Para obtener más información acerca del formato MIME, consulte RFC 2045. **Note** Este campo está presente solo si la notificación la activó una acción SNS. Las notificaciones activadas por las demás acciones no contienen este campo.

Objeto receipt

El objeto `receipt` tiene los siguientes campos.

Nombre del campo	Descripción
`action`	Objeto que encapsula información sobre la acción que se ha ejecutado. Para obtener una lista de los posibles valores, consulte Objeto action.
`dkimVerdict`	Objeto que indica si se ha superado la comprobación de DomainKeys Identified Mail

Nombre del campo	Descripción
	(DKIM). Para obtener una lista de los posibles valores, consulte Objeto dkimVerdict.
`dmarcPolicy`	Indica la configuración Domain-based Message Authentication, Reporting & Conformance (DMARC) para el dominio de envío. Este campo solo aparece si el mensaje no supera la autenticación DMARC. Los valores posibles para este campo son: • `none`: el propietario del dominio de envío solicita que no se tome ninguna medida específica para los mensajes que no superen la autenticación DMARC. • `quarantine` : el propietario del dominio de envío solicita que los receptores traten como sospechosos los mensajes que no superen la autenticación DMARC. • `reject`: el propietario del dominio de envío solicita que se rechacen los mensajes que no superen la autenticación DMARC.
`dmarcVerdict`	Objeto que indica si se ha superado la comprobación de Domain-based Message Authentication, Reporting & Conformance (DMARC). Para obtener una lista de los posibles valores, consulte Objeto dmarcVerdict.
`processingTimeMillis`	Cadena que especifica el periodo, en milisegun dos, desde el momento en que Amazon SES recibió el mensaje hasta el momento en que se desencadenó la acción.

Nombre del campo	Descripción
`recipients`	Los destinatarios (específicamente, las direcciones RCPT TO del sobre) que se corresponde con la regla de recepción activa. Las direcciones indicadas aquí pueden ser distintas de las que figuran en el campo `destination` del the section called “Objeto mail”.
`spamVerdict`	Objeto que indica si el mensaje es spam. Para obtener una lista de los posibles valores, consulte Objeto spamVerdict.
`spfVerdict`	Objeto que indica si se ha superado la comprobación de Sender Policy Framework (SPF). Para obtener una lista de los posibles valores, consulte Objeto spfVerdict.
`timestamp`	Cadena que especifica la fecha y la hora a la que se desencadenó la acción, en formato ISO 8601.
virusVerdict	Objeto que indica si el mensaje contiene un virus. Para obtener una lista de los posibles valores, consulte Objeto virusVerdict.

Objeto action

El objeto `action` tiene los siguientes campos.

Nombre del campo	Descripción
`type`	Cadena que indica el tipo de acción que se ha ejecutado. Los valores posibles son `S3`, `SNS`, `Bounce`, `Lambda`, `Stop` y `WorkMail`.

Nombre del campo	Descripción
`topicArn`	Cadena que contiene el Nombre de recurso de Amazon (ARN) del tema de Amazon SNS en el que se publicó la notificación.
`bucketName`	Cadena que contiene el nombre del bucket de Amazon S3 en el que se publicó el mensaje. Presente solo para el tipo de acción de S3.
`objectKey`	Cadena que contiene un nombre que identifica de forma única el correo electrónico en el bucket de Amazon S3. Coincide con el `messageId` del the section called “Objeto mail”. Presente solo para el tipo de acción de S3.
`smtpReplyCode`	Cadena que contiene el código de respuesta de SMTP, tal y como se define en RFC 5321. Presente solo para el tipo de acción de rebote.
`statusCode`	Cadena que contiene el código de estado mejorado de SMTP, tal y como se define en RFC 3463. Presente solo para el tipo de acción de rebote.
`message`	Cadena que contiene texto en lenguaje natural para incluir en el mensaje de rebote. Presente solo para el tipo de acción de rebote.
`sender`	Cadena que contiene la dirección de correo electrónico del remitente del correo electrónico rebotado. Esta es la dirección desde la que se envió el mensaje de rebote. Presente solo para el tipo de acción de rebote.

Nombre del campo	Descripción
`functionArn`	Cadena que contiene el ARN de la función de Lambda que se desencadenó. Presente solo para el tipo de acción Lambda.
`invocationType`	Cadena que contiene el tipo de invocación de la función de Lambda. Los posibles valores son `RequestResponse` y `Event`. Presente solo para el tipo de acción Lambda.
`organizationArn`	Cadena que contiene el ARN de la organización de Amazon WorkMail. Presente solo para el tipo de acción WorkMail.

Objeto dkimVerdict

El objeto `dkimVerdict` tiene los siguientes campos.

Nombre del campo	Descripción
`status`	Cadena que contiene el veredicto de DKIM. Los valores posibles son los siguientes: • `PASS`: el mensaje ha superado la autenticación DKIM. • `FAIL`: el mensaje no ha superado la autenticación DKIM. • `GRAY`: el mensaje no está firmado por DKIM o el dominio de origen y el dominio de firma de DKIM no coinciden. • `PROCESSING_FAILED` : hay un problema que impide que Amazon SES compruebe la firma de DKIM. Por ejemplo, las consultas de DNS devuelven un error o el encabezado de la firma DKIM no tiene el formato correcto.

Objeto dmarcVerdict

El objeto `dmarcVerdict` tiene los siguientes campos.

Nombre del campo	Descripción
`status`	Cadena que contiene el veredicto de DMARC. Los valores posibles son los siguientes: • `PASS`: el mensaje ha superado la autentica ción DMARC. • `FAIL`: el mensaje no ha superado la autenticación DMARC. • `GRAY`: al menos uno de SPF o DKIM ha superado la autenticación, pero el dominio de envío no tiene una política DMARC o utiliza la política `p=none`. • `PROCESSING_FAILED` : existe un problema que impide que Amazon SES proporcione un veredicto de DMARC.

Objeto spamVerdict

El objeto `spamVerdict` tiene los siguientes campos.

Nombre del campo	Descripción
`status`	Cadena que contiene el resultado del análisis de spam. Los valores posibles son los siguiente s: • `PASS`: el análisis de spam ha determinado que es improbable que el mensaje contenga spam. • `FAIL`: el análisis de spam ha determinado que es probable que el mensaje contenga spam.

Nombre del campo	Descripción
	• `GRAY`: Amazon SES ha analizado el correo electrónico, pero no ha podido determinar con confianza si se trata de spam. • `PROCESSING_FAILED` : Amazon SES no ha podido analizar el correo electrónico. Por ejemplo, el correo electrónico no es un mensaje MIME válido.

Objeto spfVerdict

El objeto `spfVerdict` tiene los siguientes campos.

Nombre del campo	Descripción
`status`	Cadena que contiene el veredicto de SPF. Los valores posibles son los siguientes: • `PASS`: el mensaje ha superado la autentica ción SPF. • `FAIL`: el mensaje no ha superado la autenticación SPF. • `GRAY`: el resultado del SPF es `none`, `softfail` o `neutral`. • `PROCESSING_FAILED` : hay un problema que impide que Amazon SES compruebe el registro SPF. Por ejemplo, las consultas DNS están fallando.

Objeto virusVerdict

El objeto `virusVerdict` tiene los siguientes campos.

Nombre del campo	Descripción
`status`	Cadena que contiene el resultado del análisis de virus. Los valores posibles son los siguientes: • `PASS`: el mensaje no contiene un virus. • `FAIL`: el mensaje contiene un virus. • `GRAY`: Amazon SES ha analizado el correo electrónico, pero no ha podido determinar con confianza si contiene un virus. • `PROCESSING_FAILED` : Amazon SES no puede analizar el contenido del correo electrónico. Por ejemplo, el correo electrónico no es un mensaje MIME válido.

Objeto mail

El objeto `mail` tiene los siguientes campos.

Nombre del campo	Descripción
`destination`	Lista completa de todas las direcciones de los destinatarios (incluidos en los campos To: y CC:) de los encabezados MIME de los mensajes de correo electrónico entrantes.
`messageId`	Cadena que contiene un ID único que Amazon SES asigna al correo electrónico. Si el correo electrónico se ha entregado a Amazon S3, el ID de mensaje es también la clave de objeto de Amazon S3 que se utilizó para escribir el mensaje en el bucket de Amazon S3.
`source`	Cadena que contiene la dirección de correo electrónico (específicamente, la dirección MAIL

Nombre del campo	Descripción
	FROM del sobre) desde la que se envió el correo electrónico.
`timestamp`	Cadena que contiene la hora en la que se recibió el correo electrónico, en formato ISO8601.
`headers`	Los encabezados de Amazon SES y sus encabezados personalizados. Cada encabezado tiene los siguientes campos: `name` y `value`.
`commonHeaders`	Los encabezados comunes a todos los correos electrónicos. Cada encabezado tiene los siguientes campos: `name` y `value`.
`headersTruncated`	Cadena que especifica si los encabezados se truncaron en la notificación, lo que ocurre si los encabezados tienen un tamaño superior a 10 KB. Los posibles valores son `true` y `false`.

Objeto commonHeaders

El objeto `commonHeaders` puede tener los campos que se muestran en la tabla siguiente. Los campos presentes en este objeto varían en función de los campos existentes en el correo electrónico entrante.

Nombre del campo	Descripción
`messageId`	El ID del mensaje original.
`date`	La fecha y hora en que Amazon SES recibió el mensaje.
`to`	El encabezado To del correo electrónico.
`cc`	El encabezado CC del correo electrónico.

Nombre del campo	Descripción
`bcc`	El encabezado BCC del correo electrónico.
`from`	El encabezado From del correo electrónico.
`sender`	El encabezado Sender del correo electrónico.
`returnPath`	El encabezado Return-Path del correo electrónico.
`replyTo`	El encabezado Reply-To del correo electrónico.
`subject`	El encabezado Subject del correo electrónico.

Ejemplos de notificaciones para recepción de correo electrónico de Amazon SES

En esta sección, se ofrecen ejemplos de los siguientes tipos de notificaciones:

- Una notificación enviada como resultado de una acción de SNS.
- Una notificación enviada como resultado de otro tipo de acción (una notificación de alerta).

Notificación de una acción de SNS

Esta sección contiene un ejemplo de una notificación de acción de SNS. A diferencia de la notificación de alerta mostrada anteriormente, incluye una sección `content` que contiene el correo electrónico, que suele estar en formato Multipurpose Internet Mail Extensions (MIME).

```
{
  "notificationType":"Received",
  "receipt":{
    "timestamp":"2015-09-11T20:32:33.936Z",
    "processingTimeMillis":222,
    "recipients":[
      "recipient@example.com"
    ],
    "spamVerdict":{
      "status":"PASS"
    },
    "virusVerdict":{
```

```
      "status":"PASS"
    },
    "spfVerdict":{
      "status":"PASS"
    },
    "dkimVerdict":{
      "status":"PASS"
    },
    "action":{
      "type":"SNS",
      "topicArn":"arn:aws:sns:us-east-1:012345678912:example-topic"
    }
  },
  "mail":{
    "timestamp":"2015-09-11T20:32:33.936Z",
    "source":"61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com",
    "messageId":"d6iitobk75ur44p8kdnnp7g2n800",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "headers":[
      {
        "name":"Return-Path",

 "value":"<0000014fbe1c09cf-7cb9f704-7531-4e53-89a1-5fa9744f5eb6-000000@amazonses.com>"
      },
      {
        "name":"Received",
        "value":"from a9-183.smtp-out.amazonses.com (a9-183.smtp-out.amazonses.com
 [54.240.9.183]) by inbound-smtp.us-east-1.amazonaws.com with SMTP id
 d6iitobk75ur44p8kdnnp7g2n800 for recipient@example.com; Fri, 11 Sep 2015 20:32:33
 +0000 (UTC)"
      },
      {
        "name":"DKIM-Signature",
        "value":"v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple;
 s=ug7nbtf4gccmlpwj322ax3p6ow6yfsug; d=amazonses.com; t=1442003552;
 h=From:To:Subject:MIME-Version:Content-Type:Content-Transfer-Encoding:Date:Message-
ID:Feedback-ID; bh=DWr3IOmYWoXCA9ARqGC/UaODfghffiwFNRIb2Mckyt4=;
 b=p4ukUDSFqhqiub+zPR0DW1kp7oJZakrzupr6LBe6sUuvqpBkig56UzUwc29rFbJF
 hlX3Ov7DeYVNoN38stqwsF8ivcajXpQsXRC1cW9z8x875J041rClAjV7EGbLmudVpPX
 4hHst1XPyX5wmgdHIhmUuh8oZKpVqGi6bHGzzf7g="
      },
```

```
      {
        "name":"From",
        "value":"sender@example.com"
      },
      {
        "name":"To",
        "value":"recipient@example.com"
      },
      {
        "name":"Subject",
        "value":"Example subject"
      },
      {
        "name":"MIME-Version",
        "value":"1.0"
      },
      {
        "name":"Content-Type",
        "value":"text/plain; charset=UTF-8"
      },
      {
        "name":"Content-Transfer-Encoding",
        "value":"7bit"
      },
      {
        "name":"Date",
        "value":"Fri, 11 Sep 2015 20:32:32 +0000"
      },
      {
        "name":"Message-ID",
        "value":"<61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>"
      },
      {
        "name":"X-SES-Outgoing",
        "value":"2015.09.11-54.240.9.183"
      },
      {
        "name":"Feedback-ID",
        "value":"1.us-east-1.Krv2FKpFdWV+KUYw3Qd6wcpPJ4Sv/pOPpEPSHn2u2o4=:AmazonSES"
      }
    ],
    "commonHeaders":{

  "returnPath":"0000014fbe1c09cf-7cb9f704-7531-4e53-89a1-5fa9744f5eb6-000000@amazonses.com",
```

```
      "from":[
        "sender@example.com"
      ],
      "date":"Fri, 11 Sep 2015 20:32:32 +0000",
      "to":[
        "recipient@example.com"
      ],
      "messageId":"<61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>",
      "subject":"Example subject"
    }
  },
  "content":"Return-Path: <61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>\r
\nReceived: from a9-183.smtp-out.amazonses.com (a9-183.smtp-out.amazonses.com
 [54.240.9.183])\r\n by inbound-smtp.us-east-1.amazonaws.com with SMTP id
 d6iitobk75ur44p8kdnnp7g2n800\r\n for recipient@example.com;\r\n Fri, 11 Sep 2015
 20:32:33 +0000 (UTC)\r\nDKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/
simple;\r\n\ts=ug7nbtf4gccmlpwj322ax3p6ow6yfsug; d=amazonses.com; t=1442003552;\r\n
\th=From:To:Subject:MIME-Version:Content-Type:Content-Transfer-Encoding:Date:Message-
ID:Feedback-ID;\r\n\tbh=DWr3IOmYWoXCA9ARqGC/UaODfghffiwFNRIb2Mckyt4=;\r\n
\tb=p4ukUDSFqhqiub+zPR0DW1kp7oJZakrzupr6LBe6sUuvqpBkig56UzUwc29rFbJF\r\n
\thlX3Ov7DeYVNoN38stqwsF8ivcajXpQsXRC1cW9z8x875J041rClAjV7EGbLmudVpPX\r\n
\t4hHst1XPyX5wmgdHIhmUuh8oZKpVqGi6bHGzzf7g=\r\nFrom: sender@example.com\r\nTo:
 recipient@example.com\r\nSubject: Example subject\r\nMIME-Version: 1.0\r\nContent-
Type: text/plain; charset=UTF-8\r\nContent-Transfer-Encoding: 7bit\r\nDate: Fri, 11 Sep
 2015 20:32:32 +0000\r\nMessage-ID: <61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>
\r\nX-SES-Outgoing: 2015.09.11-54.240.9.183\r\nFeedback-ID: 1.us-east-1.Krv2FKpFdWV
+KUYw3Qd6wcpPJ4Sv/pOPpEPSHn2u2o4=:AmazonSES\r\n\r\nExample content\r\n"
}
```

Notificación de alerta

Esta sección contiene un ejemplo de una notificación de Amazon SNS que se puede desencadenar mediante una acción de S3. Las notificaciones desencadenadas por acciones de Lambda, acciones de rebote, acciones de detención y acciones de WorkMail son similares. Aunque la notificación contiene información sobre el correo electrónico, no incluye el contenido del propio correo electrónico.

```
{
"notificationType": "Received",
"receipt": {
"timestamp": "2015-09-11T20:32:33.936Z",
"processingTimeMillis": 406,
"recipients": [
```

```
 "recipient@example.com"
],
"spamVerdict": {
 "status": "PASS"
},
"virusVerdict": {
 "status": "PASS"
},
"spfVerdict": {
 "status": "PASS"
},
"dkimVerdict": {
 "status": "PASS"
},
"action": {
 "type": "S3",
 "topicArn": "arn:aws:sns:us-east-1:012345678912:example-topic",
 "bucketName": "my-S3-bucket",
 "objectKey": "\email"
}
},
"mail": {
"timestamp": "2015-09-11T20:32:33.936Z",
"source": "0000014fbe1c09cf-7cb9f704-7531-4e53-89a1-5fa9744f5eb6-000000@amazonses.com",
"messageId": "d6iitobk75ur44p8kdnnp7g2n800",
"destination": [
 "recipient@example.com"
],
"headersTruncated": false,
"headers": [
 {
  "name": "Return-Path",
  "value":
 "<0000014fbe1c09cf-7cb9f704-7531-4e53-89a1-5fa9744f5eb6-000000@amazonses.com>"
 },
 {
  "name": "Received",
  "value": "from a9-183.smtp-out.amazonses.com (a9-183.smtp-out.amazonses.com
 [54.240.9.183]) by inbound-smtp.us-east-1.amazonaws.com with SMTP id
 d6iitobk75ur44p8kdnnp7g2n800 for recipient@example.com; Fri, 11 Sep 2015 20:32:33
 +0000 (UTC)"
 },
 {
  "name": "DKIM-Signature",
```

```
  "value": "v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple;
 s=ug7nbtf4gccmlpwj322ax3p6ow6yfsug; d=amazonses.com; t=1442003552;
 h=From:To:Subject:MIME-Version:Content-Type:Content-Transfer-Encoding:Date:Message-
ID:Feedback-ID; bh=DWr3IOmYWoXCA9ARqGC/UaODfghffiwFNRIb2Mckyt4=;
 b=p4ukUDSFqhqiub+zPR0DW1kp7oJZakrzupr6LBe6sUuvqpBkig56UzUwc29rFbJF
 hlX3Ov7DeYVNoN38stqwsF8ivcajXpQsXRC1cW9z8x875J041rClAjV7EGbLmudVpPX
 4hHst1XPyX5wmgdHIhmUuh8oZKpVqGi6bHGzzf7g="
 },
 {
  "name": "From",
  "value": "sender@example.com"
 },
 {
  "name": "To",
  "value": "recipient@example.com"
 },
 {
  "name": "Subject",
  "value": "Example subject"
 },
 {
  "name": "MIME-Version",
  "value": "1.0"
 },
 {
  "name": "Content-Type",
  "value": "text/plain; charset=UTF-8"
 },
 {
  "name": "Content-Transfer-Encoding",
  "value": "7bit"
 },
 {
  "name": "Date",
  "value": "Fri, 11 Sep 2015 20:32:32 +0000"
 },
 {
  "name": "Message-ID",
  "value": "<61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>"
 },
 {
  "name": "X-SES-Outgoing",
  "value": "2015.09.11-54.240.9.183"
 },
```

```
 {
  "name": "Feedback-ID",
  "value": "1.us-east-1.Krv2FKpFdWV+KUYw3Qd6wcpPJ4Sv/pOPpEPSHn2u2o4=:AmazonSES"
 }
],
"commonHeaders": {
 "returnPath":
 "0000014fbe1c09cf-7cb9f704-7531-4e53-89a1-5fa9744f5eb6-000000@amazonses.com",
 "from": [
  "sender@example.com"
 ],
 "date": "Fri, 11 Sep 2015 20:32:32 +0000",
 "to": [
  "recipient@example.com"
 ],
 "messageId": "<61967230-7A45-4A9D-BEC9-87CBCF2211C9@example.com>",
 "subject": "Example subject"
}
}
}
```

Acción de detención del conjunto de reglas

La acción Stop (Detener) termina la evaluación del conjunto de reglas de recepción y, opcionalmente, lo notifica a través de Amazon SNS. Esta acción tiene las siguientes opciones.

- SNS Topic (Tema de SNS): el nombre o ARN del tema de Amazon SNS al que se enviará la notificación cuando se ejecute la acción Stop (Detener). Un ejemplo de un ARN de tema de Amazon SNS es: arn:aws:sns:us-east-1:123456789012:MyTopic. Para crear un tema de Amazon SNS al configurar la acción puede elegir Create SNS Topic (Crear tema de SNS). Para obtener más información acerca de los temas de Amazon SNS, consulte la Guía para desarrolladores de Amazon Simple Notification Service.

  > **Note**
  >
  > El tema de Amazon SNS que elija deberá estar en la misma región de AWS que el punto de conexión de Amazon SES que utilice para recibir correo electrónico.

Acción de integración con Amazon WorkMail

La acción de WorkMail se integra con Amazon WorkMail. Si Amazon WorkMail realiza todo el procesamiento del correo electrónico, normalmente no utilizará esta acción de manera directa, ya que Amazon WorkMail se encarga de la configuración. Esta acción tiene las siguientes opciones.

- Organization ARN (ARN de la organización): el ARN de la organización de Amazon WorkMail. Los ARN de la organización de Amazon WorkMail tienen la forma `arn:aws:workmail:`*`region`*`:`*`account_ID`*`:organization/`*`organization_ID`*, donde:
  - `region` es la región en la que utiliza Amazon SES y Amazon WorkMail. (Debe utilizarlos desde la misma región). Por ejemplo, us-east-1.
  - `account_ID` es el ID de cuenta de AWS. Puede encontrar su ID de cuenta de AWS en la página Account (Cuenta) de la consola de administración de AWS.
  - `organization_ID` es un identificador único que genera Amazon WorkMail cuando se crea una organización. Puede encontrar el ID de la organización en la consola de Amazon WorkMail en la página Organization Settings (Configuración de la organización) de su organización.

  Un ejemplo de ARN de la organización de Amazon WorkMail completo es arn:aws:workmail:us-east-1:123456789012:organization/m-68755160c4cb4e29a2b2f8fb58f359d7. Para obtener más información sobre las organizaciones de Amazon WorkMail, consulte la Guía del administrador de Amazon WorkMail.
- SNS Topic (Tema de SNS): el nombre o ARN del tema de Amazon SNS al que se enviará una notificación cuando se ejecute la acción de Amazon WorkMail. Un ejemplo de un ARN de tema de Amazon SNS es: arn:aws:sns:us-east-1:123456789012:MyTopic. Para crear un tema de Amazon SNS al configurar la acción, puede elegir Create SNS Topic (Crear tema de SNS). Para obtener más información acerca de los temas de Amazon SNS, consulte la Guía para desarrolladores de Amazon Simple Notification Service.

> **Note**
>
> El tema de Amazon SNS que elija deberá estar en la misma región de AWS que el punto de conexión de Amazon SES que utilice para recibir correo electrónico.

> **Note**
>
> Amazon SES solo admite las acciones de WorkMail en las regiones en las que WorkMail esté disponible. Consulte Puntos de enlace y cuotas de Amazon WorkMail en la Referencia general de AWS.

Explicación de la consola de creación de filtros de direcciones IP

Esta sección le guiará a través de la configuración de filtros de direcciones IP mediante la consola de Amazon SES. El filtrado de direcciones IP le permite proporcionar un amplio nivel de control. Estos filtros de IP permiten bloquear o permitir explícitamente todos los mensajes de direcciones IP o rangos de direcciones IP específicos.

De forma opcional, puede utilizar la API de `CreateReceiptFilter` para crear un filtro de direcciones IP, tal como se describe en la Referencia de la API de Amazon Simple Email Service.

> **Note**
>
> Si solo desea recibir emails de una lista finita de direcciones IP conocidas, entonces configure una lista de bloques que contenga `0.0.0.0/0` y configure una lista permitida que contenga las direcciones IP de confianza. Esta configuración bloquea todas las direcciones IP de forma predeterminada y solo permite correo de las direcciones IP que especifique de forma explícita.

Requisitos previos

Se deben cumplir los siguientes requisitos previos para continuar con la configuración del control de correo electrónico basado en destinatarios mediante los filtros de direcciones IP:

1. En primer lugar, debe crear y verificar una identidad de dominio en Amazon SES.
2. A continuación, debe especificar qué servidores de correo pueden aceptar correo para su dominio mediante la publicación de un registro MX en la configuración de DNS de su dominio. (El registro MX debe hacer referencia al punto de enlace de Amazon SES que recibe correo electrónico para la región de AWS en la que se utiliza Amazon SES).

Creación de filtros de direcciones IP

Para crear un filtro de direcciones IP mediante la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación izquierdo, elija Email Receiving (Recepción de correo electrónico).
3. Seleccione la pestaña IP address filters (Filtros de direcciones IP).
4. Elija Create Filter.
5. Ingrese un nombre único para el filtro: la leyenda del campo indicará los requisitos de sintaxis. El nombre debe contener menos de 64 caracteres alfanuméricos, guiones (-), guiones bajos (_) y puntos (.). El nombre debe comenzar y terminar con una letra o un número.
6. Ingrese una dirección IP o un intervalo de direcciones IP: la leyenda del campo proporcionará ejemplos especificados en la sintaxis de enrutamiento entre dominios sin clases (CIDR). Un ejemplo de dirección IP única es 10.0.0.1. Un ejemplo de rango de direcciones IP es 10.0.0.1/24. Para obtener más información acerca de la notación CIDR, consulteRFC 2317.
7. Elija el valor de Policy type (Tipo de política). Seleccione el botón de opción Block (Bloquear) o Allow (Permitir).
8. Elija Create Filter (Crear filtro).
9. Si desea agregar otro filtro de IP, elija Create filter (Crear filtro) y repita los pasos anteriores para cada filtro adicional que desee agregar.
10. Si desea eliminar un filtro de dirección IP, selecciónelo y elija el botón Delete (Eliminar).

Visualización de métricas para la recepción de emails de Amazon SES

Si has activado la recepción de correos electrónicos en Amazon SES y has creado reglas de recepción para tu correo electrónico, puedes ver las métricas de esos conjuntos de reglas y reglas de recepción a través de Amazon CloudWatch.

En la CloudWatch consola, encontrarás las métricas en Métricas > Todas las métricas > SES > Métricas del conjunto de reglas de recepción y Métricas de reglas de recepción.

> **Note**
>
> Las métricas del conjunto de reglas de recepción y las métricas de reglas de recepción no aparecerán en SES si todavía no ha:
>
> - habilitado la recepción de correo electrónico
> - creado las reglas de recepción
> - recibido ningún correo que coincida con alguna de las reglas.

Las métricas del mensaje siguiente están disponibles:

- Recepción de mensajes

Ámbito	Métrica	Descripción	Dimensión
Métricas de conjunto de reglas de recepción	Recibido	SES recibió correctamente un mensaje al que se le aplica al menos una regla. Esta métrica solo puede tener un valor de 1.	RuleSetName
Métricas de reg	Recibido	SES recibió correctamente un mensaje e intentará procesar la regla aplicada. Esta métrica solo puede tener un valor de 1.	RuleName

- Publicación de mensajes

Ámbito	Métrica	Descripción	Dimensión
Métricas de cor	PublishSuccess	SES ejecutó correctamente todas las reglas que se aplican dentro de un conjunto de reglas.	RuleSetName
Métricas de reg	PublishSuccess	SES ejecutó correctamente una regla que se aplica al mensaje de recepción.	RuleName

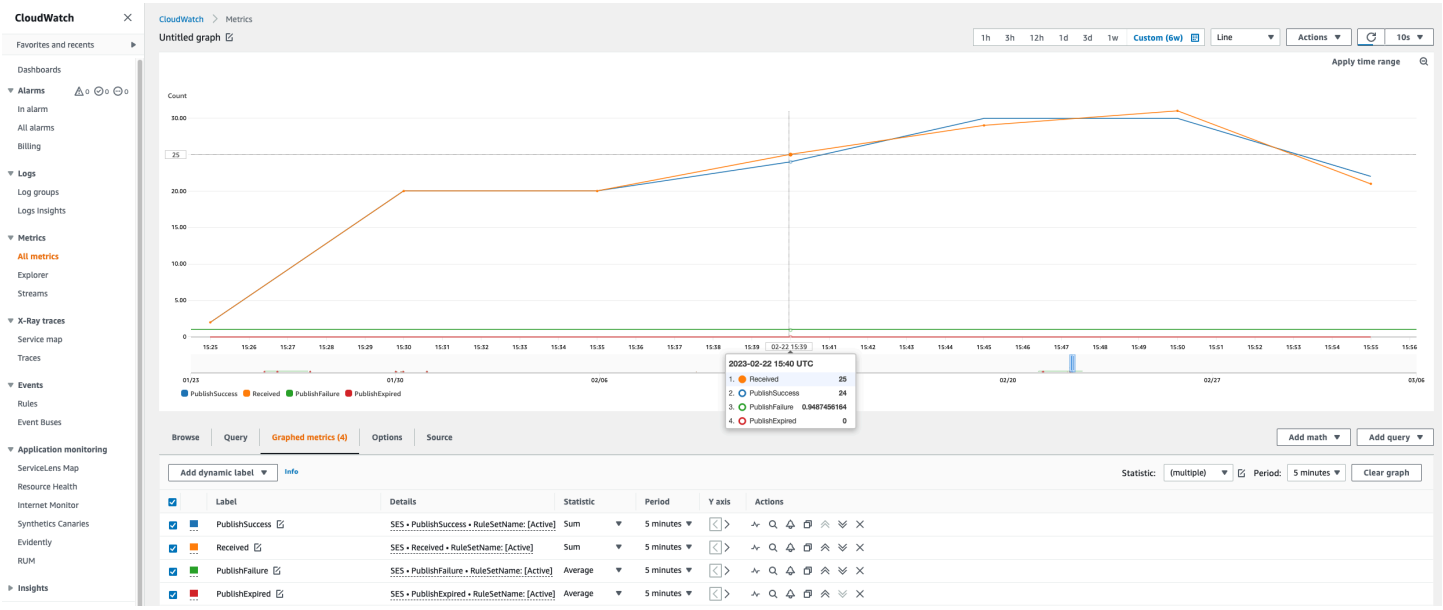
Ámbito	Métrica	Descripción	Dimensión
Métricas del co	PublishFailure	SES detectó un error al intentar ejecutar reglas dentro de un conjunto de reglas. Se volverá a intentar la ejecución.	RuleSetName
Métricas de reg	PublishFailure	SES detectó un error al intentar ejecutar las acciones en una regla; en función del error, es posible que se vuelva a intentar la ejecución.	RuleName
Métricas del co	PublishExpired	SES ya no volverá a intentar ejecutar las reglas porque no se ejecutaron correctamente en un plazo de 36 horas o porque detectó un error irrecuperable.	RuleSetName
Métricas de reg	PublishExpired	SES ya no volverá a intentar ejecutar las acciones de la regla porque no se ejecutaron correctamente en un plazo de 36 horas.	RuleName

Note

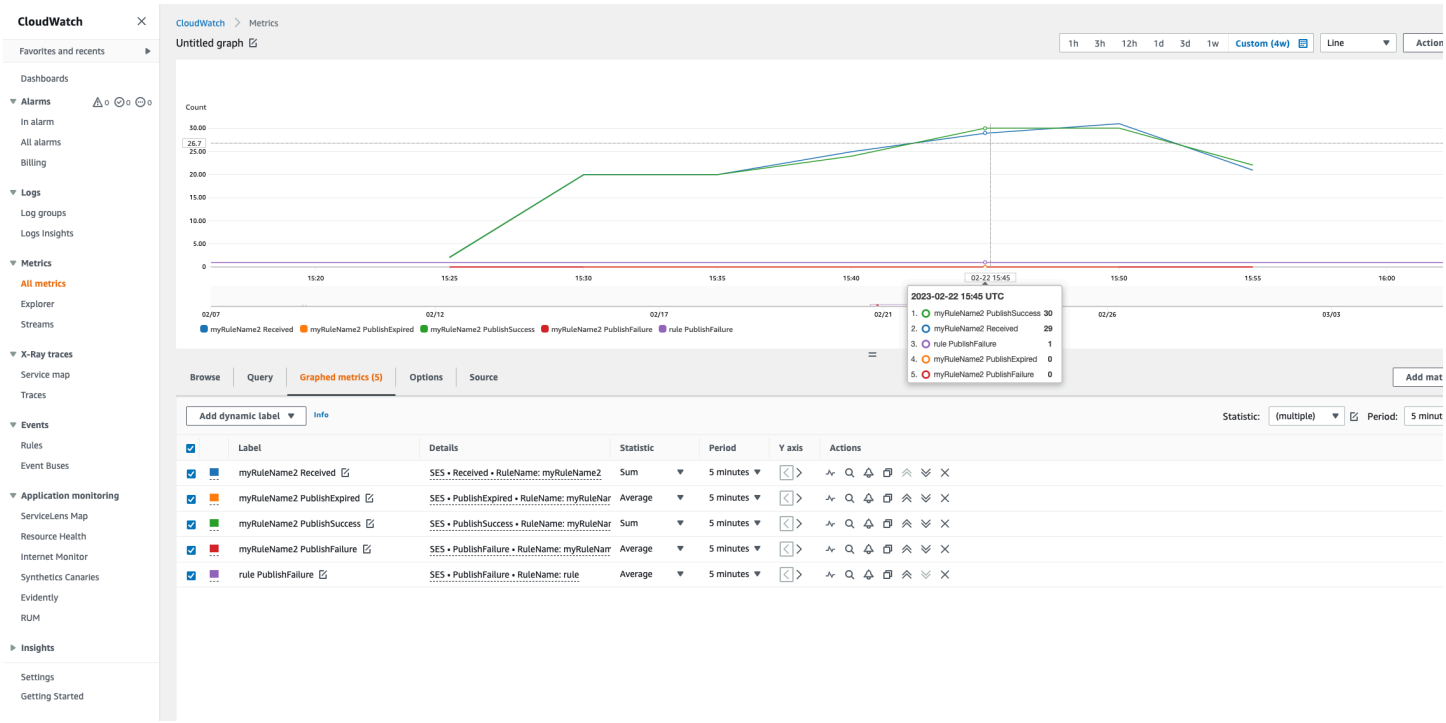
- En las tablas anteriores, el término aplica significa que el remitente no está en la lista de bloqueo de filtros de IP ni está en la lista de bloqueo interna de SES y que la regla tiene condiciones de destinatario coincidentes y una política de TLS coincidentes.
- Se pueden producir errores de publicación, por ejemplo, si eliminó o revocó permisos para un bucket de Amazon S3, un tema de Amazon SNS o una función de Lambda que una acción de una de las reglas de recepción utilizaba según lo establecido en su configuración.
- Como solo puede estar activo un conjunto de reglas a la vez, SES publica una métrica agregada que se muestra como RuleSetName: [Activa] para todos los conjuntos de reglas que estuvieron activos durante el intervalo de tiempo que usted seleccione. CloudWatch Esto tiene la ventaja de que le permite cambiar libremente los conjuntos de reglas sin ningún cambio en la configuración de alarma.

> **Important**
>
> Los cambios que introduzca para corregir el conjunto de reglas de recepción se aplicarán solo a los emails que Amazon SES reciba después de la actualización. Los correos electrónicos siempre se evalúan respecto al conjunto de reglas de recepción en vigor en el momento en que se recibió el correo electrónico.

Las métricas de un conjunto de reglas de recepción de SES se muestran en la CloudWatch consola.



Las métricas de una regla de recepción de SES se muestran en la CloudWatch consola.


CloudWatch
Favorites and recents
Dashboards
Alarms
In alarm
All alarms
Billing
Logs
Log groups
Logs Insights
Metrics
All metrics
Explorer
Streams
X-Ray traces
Service map
Traces
Events
Rules
Event Buses
Application monitoring
ServiceLens Map
Resource Health
Internet Monitor
Synthetics Canaries
Evidently
RUM
Insights
Settings
Getting Started
CloudWatch > Metrics
Untitled graph
1h 3h 12h 1d 3d 1w Custom (4w)
Line
Count
2023-02-22 15:45 UTC
1. myRuleName2 PublishSuccess 30
2. myRuleName2 Received 29
3. rule PublishFailure 1
4. myRuleName2 PublishExpired 0
5. myRuleName2 PublishFailure 0
myRuleName2 Received
myRuleName2 PublishExpired
myRuleName2 PublishSuccess
myRuleName2 PublishFailure
rule PublishFailure
Browse
Query
Graphed metrics (5)
Options
Source
Add dynamic label
Info
Statistic:
(multiple)
Period:
5 minut
Label
Details
Statistic
Period
Y axis
Actions
myRuleName2 Received
SES • Received • RuleName: myRuleName2
Sum
5 minutes
myRuleName2 PublishExpired
SES • PublishExpired • RuleName: myRuleNar
Average
myRuleName2 PublishSuccess
SES • PublishSuccess • RuleName: myRuleNar
myRuleName2 PublishFailure
SES • PublishFailure • RuleName: myRuleNam
rule PublishFailure
SES • PublishFailure • RuleName: rule

Identidades verificadas en Amazon SES

En Amazon SES, una identidad verificada es un dominio o una dirección de correo electrónico que se utiliza para enviar o recibir correo electrónico. Para poder enviar un correo electrónico mediante Amazon SES, debe crear y verificar cada identidad que va a utilizar como dirección en los campos “From”, “Source”, “Sender” o “Return-Path”. Al verificar una identidad con Amazon SES, confirma que es de su propiedad y ayuda a evitar el uso no autorizado.

Si su cuenta aún está en el entorno aislado de Amazon SES, también debe verificar las direcciones de correo electrónico a las que planea enviar correo, a menos que envíe a las bandejas de entrada de prueba proporcionadas por el simulador de buzón de correo de Amazon SES. Para obtener más información, consulte the section called “Uso del simulador de buzón de correo de forma manual”.

Puede crear una identidad mediante la consola de Amazon SES o la API de Amazon SES. El proceso de verificación de identidad depende del tipo de identidad que elija crear.

> **Tip**
>
> Si es la primera vez que usa SES, puede usar el asistente de introducción para crear y verificar la primera identidad (dirección de correo electrónico o dominio).

Contenido

- Creación y verificación de identidades en Amazon SES
- Administración de identidades en Amazon SES
- Configuración de identidades en Amazon SES
- Envío de correos electrónicos de prueba en Amazon SES con el simulador

Creación y verificación de identidades en Amazon SES

En Amazon SES, puede crear una identidad de nivel de dominio o puede crear una identidad de dirección de correo electrónico. Estos tipos de identidades no son mutuamente excluyentes. En la mayoría de los casos, la creación de una identidad de dominio elimina la necesidad de crear y verificar identidades de direcciones de correo electrónico individuales, a menos que desee aplicar configuraciones personalizadas a una dirección de correo electrónico específica. Tanto si crea un

dominio y utiliza direcciones de correo electrónico basadas en el dominio, como si crea direcciones de correo electrónico individuales, ambos enfoques presentan beneficios. El método que elija depende de sus necesidades específicas, como se explica a continuación.

Crear y verificar una identidad de dirección de correo electrónico es la forma más rápida de comenzar a trabajar en SES, pero la verificación de una identidad a nivel de dominio ofrece ventajas. Cuando verifica una identidad de dirección de correo electrónico, solo puede usarse esa dirección para enviar correo electrónico, pero cuando verifica la identidad de un dominio, puede enviar correos desde cualquier subdominio o dirección de correo electrónico del dominio verificado sin tener que verificar cada uno de ellos de forma individual. Por ejemplo, si crea y verifica la identidad de un dominio denominado example.com, no es necesario que cree identidades de subdominio separadas para a.example.com, a.b.example.com, ni identidades de dirección de correo electrónico separadas para user@example.com, user@a.example.com, etc.

Sin embargo, tenga en cuenta que una identidad de dirección de correo electrónico que utiliza la verificación heredada de su dominio se limita al envío directo de correo electrónico. Si quiere realizar envíos más avanzados, también tendrá que verificarlo explícitamente como una identidad de dirección de correo electrónico. El envío avanzado incluye el uso de la dirección de correo electrónico con conjuntos de configuraciones, autorizaciones de políticas para el envío delegado y configuraciones que anulan la configuración del dominio.

Para ayudar a aclarar las capacidades de herencia de verificación y envío de correo electrónico analizadas anteriormente, la siguiente tabla clasifica cada combinación de verificación de dominio/dirección de correo electrónico y enumera la herencia, el nivel de envío y el estado de visualización de cada una:

	Solo dominio verificado	Solo dirección de correo electrónico verificada	Verificación del dominio y la dirección de correo electrónico
Nivel de herencia	Verificación heredada de subdominios y direcciones de correo electrónico del dominio principal.	Dirección de correo electrónico verificada explícitamente.	• Verificación heredada de subdominios del dominio principal. • Dirección de correo electrónico verificada explícitamente.

	Solo dominio verificado	Solo dirección de correo electrónico verificada	Verificación del dominio y la dirección de correo electrónico
Nivel de envío	Direcciones de correo electrónico limitadas al envío directo de correo electrónico.	La dirección de correo electrónico se puede utilizar en el envío avanzado*.	La dirección de correo electrónico se puede utilizar en el envío avanzado*.
Estado mostrado	Estado de la consola/API: • Dominio/subdominios = Verificado • Dirección de correo electrónico = sin verificar.	Estado de la consola/API: • Dirección de correo electrónico = verificada	Estado de la consola/API: • Dominio/subdominios = Verificado • Dirección de correo electrónico = verificada.

*El envío avanzado incluye el uso de la dirección de correo electrónico con conjuntos de configuraciones, autorizaciones de políticas para el envío delegado y configuraciones que anulan la configuración del dominio.

Para enviar correo electrónico desde el mismo dominio o dirección de correo electrónico en más de una Región de AWS, debe crear y verificar una identidad de forma independiente para cada región. Puede verificar hasta 10 000 identidades en cada región.

Al crear y verificar identidades de dirección de correo electrónico y dominio, tenga en cuenta lo siguiente:

- Puede enviar correo electrónico desde cualquier subdominio o dirección de correo electrónico del dominio verificado sin tener que verificar cada uno de ellos de forma individual. Por ejemplo, si crea y verifica una identidad para example.com, no es necesario que cree identidades separadas para a.example.com, a.b.example.com, user@example.com, user@a.example.com, etc.
- Tal como se especifica en RFC 1034, cada etiqueta de DNS puede tener hasta 63 caracteres y el nombre de dominio completo no debe superar una longitud total de 255 caracteres.

- Si verifica un dominio, subdominio o dirección de correo electrónico que compartan un dominio raíz, la configuración de identidad (como, por ejemplo, las notificaciones de retroalimentación) se aplican al nivel más pormenorizado que haya verificado.
  - La configuración de identidad de dirección de correo electrónico verificada sobrescribe la configuración de identidad de dominio verificada.
  - La configuración de identidad de subdominio verificada anula la configuración de identidad de dominio verificada, las configuraciones de subdominio de nivel inferior sobrescriben las configuraciones de subdominio de nivel superior.

    Por ejemplo, imagine que verifica usuario@a.b.example.com, a.b.example.com, b.example.com y example.com. Esta es la configuración de identidad verificada que se utilizará en los siguientes casos:
    - Los correos electrónicos enviados desde user@example.com (una dirección de correo electrónico que no se ha verificado específicamente) utilizarán la configuración para example.com.
    - Los correos electrónicos enviados desde usuario@a.b.example.com (una dirección de correo electrónico que se ha verificado específicamente) utilizarán la configuración para usuario@a.b.example.com.
    - Los correos electrónicos enviados desde user@b.example.com (una dirección de correo electrónico que no se ha verificado específicamente) utilizarán la configuración para b.example.com.
- Puede añadir etiquetas a las direcciones de correo electrónico verificadas sin necesidad de realizar pasos de verificación adicionales. Para añadir una etiqueta a una dirección de correo electrónico, añada un signo más (+) entre la cuenta y el signo "arroba" (@), seguido por una etiqueta de texto. Por ejemplo, si ya ha verificado sender@example.com, puede utilizar sender+myLabel@example.com como dirección "From" o "Return-Path" de sus correos electrónicos. Puede utilizar esta característica para implementar la ruta variable de retorno de sobres (VERP). A continuación, puede utilizar VERP para detectar y eliminar de sus listas de correo las direcciones de correo electrónico que generan errores de entrega.
- Los nombres de dominio no distinguen entre mayúsculas y minúsculas. Si verifica example.com, puede enviar desde EXAMPLE.com también.
- Las direcciones de correo electrónico distinguen entre mayúsculas y minúsculas. Si verifica sender@EXAMPLE.com, no puede enviar correo electrónico desde sender@example.com a menos que verifique también sender@example.com.

- En cada Región de AWS, puede verificar hasta 10 000 identidades (dominios y direcciones de correo electrónico en cualquier combinación).

> **Tip**
>
> Si es la primera vez que usa SES, puede usar el asistente de introducción para crear y verificar la primera identidad (dirección de correo electrónico o dominio).

Contenido

- Creación de una identidad de dominio
- Verificación de una identidad de dominio DKIM con el proveedor de DNS
- Creación de una identidad de dirección de correo electrónico
- Verificación de una identidad de dirección de correo electrónico
- Crear y verificar una identidad y asignar un conjunto de configuración predeterminado al mismo tiempo
- Uso de plantillas de correo electrónico de verificación personalizado

Creación de una identidad de dominio

Parte de la creación de una identidad de dominio consiste en configurar su verificación basada en DKIM. DomainKeys Identified Mail (DKIM) es un método de autenticación de correo electrónico que utiliza Amazon SES para verificar la propiedad del dominio y que los servidores receptores de correo utilizan para validar la autenticidad del correo electrónico. Puede configurar DKIM mediante Easy DKIM o Bring Your Own DKIM (BYODKIM) (Utilice su propio DKIM). Dependiendo de su elección, tendrá que configurar la longitud de la clave de firma de la clave privada de la siguiente manera:

- Easy DKIM: acepte el valor predeterminado de Amazon SES de 2048 bits o sobrescríbalo al seleccionar la opción de 1024 bits.
- BYODKIM: la longitud de la clave privada debe ser de al menos 1024 bits y puede ser de hasta 2048 bits.

Consulte the section called “Longitud de clave de firma de DKIM” para obtener más información acerca de las longitudes de clave de firma DKIM y cómo cambiarlas.

En el siguiente procedimiento se muestra cómo crear una identidad de dominio mediante la consola de Amazon SES.

- Si ya creó el dominio y solo necesita verificarlo, pase al procedimiento the section called “Verificación de una identidad de dominio” en esta página.

Para crear una identidad de dominio

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).
3. Elija Create identity (Crear identidad).
4. En Identity details (Detalles de la identidad), seleccione Domain (Dominio) como el tipo de identidad que desea crear. Para completar el proceso de verificación de dominio, debe tener acceso a la configuración de DNS del dominio.
5. Ingrese el nombre del dominio o subdominio en el campo Domain (Dominio).

   > **Tip**
   >
   > Si su dominio es www.ejemplo.com, escriba ejemplo.com como su dominio. No incluya “www.”, ya que, de lo contrario, el proceso de verificación del dominio no se realizará correctamente.

6. (Opcional) Si desea Asignar un conjunto de configuración predeterminado, active la casilla de verificación.

   1. Para Default configuration set (Conjunto de configuración predeterminado), seleccione el conjunto de configuración existente que desee asignar a su identidad. Si aún no ha creado ningún conjunto de configuración, consulte Conjuntos de configuración.

      > **Note**
      >
      > Amazon SES solo toma el conjunto de configuración asignado de manera predeterminada cuando no se especifica ningún otro conjunto en el momento del

envío. Si se especifica un conjunto de configuración, Amazon SES aplica el conjunto especificado en lugar del predeterminado.

7. (Opcional) Si desea Utilizar un dominio MAIL FROM personalizado, active la casilla de verificación y realice los pasos siguientes. Para obtener más información, consulte the section called “Uso de un dominio MAIL FROM personalizado”.

   1. En MAIL FROM domain, escriba el subdominio que desea utilizar como dominio MAIL FROM. Debe ser un subdominio de la identidad de dominio que se está verificando. El dominio MAIL FROM no debe ser un dominio desde el que se envíe correo electrónico.
   2. Para Behaviour on MX failure (Comportamiento ante error de MX), indique qué acción debe realizar Amazon SES si no encuentra el registro MX requerido en el momento del envío. Elija una de las siguientes opciones:
      - Use default MAIL FROM domain (Utilizar dominio MAIL FROM predeterminado): si el registro MX del dominio MAIL FROM personalizado no se ha configurado correctamente, Amazon SES utilizará un subdominio de amazonses.com. El subdominio varía en función de la Región de AWS en la que se utilice Amazon SES.
      - Rechazar mensaje: si el registro MX del dominio MAIL FROM personalizado no está configurado correctamente, Amazon SES devolverá un error `MailFromDomainNotVerified`. Si elige esta opción, los mensajes de correo electrónico que intente enviar desde este dominio se rechazarán automáticamente.
   3. ParaPublish DNS records to Route 53 (Publicar registros DNS en Route 53), si su dominio está alojado a través de Amazon Route 53, tiene la opción de permitir que SES publique los registros TXT y MX asociados en el momento de la creación al marcar Enabled (Habilitado). Si prefiere publicar estos registros más tarde, desmarque la casilla de verificación Enabled (Habilitado). (Puede volver más tarde para publicar los registros en Route 53 al editar la identidad; consulte the section called “Edición de una identidad mediante la consola”.)

8. (Opcional) Para configurar la verificación personalizada basada en DKIM fuera de la configuración predeterminada de SES que utiliza Easy DKIM con una longitud de canto de 2048 bits, en Verifying your domain (Verificación de su dominio), expanda Advanced DKIM settings (Configuración avanzada de DKIM) y elija el tipo de DKIM que desea configurar:

   a. Easy DKIM:

      i. En el campo Identity type (Tipo de identidad), elija Easy DKIM.

ii. En el campo DKIM signing key length (Longitud de clave de firma de DKIM), elija RSA_2048_BIT o RSA_1024_BIT.

iii. Para Publish DNS records to Route 53 (Publicar registros DNS en Route 53), si su dominio está alojado a través de Amazon Route 53, tiene la opción de permitir que SES publique los registros CNAME asociados en el momento de la creación al marcar Enabled (Habilitado). Si prefiere publicar estos registros más tarde, desmarque la casilla de verificación Enabled (Habilitado). (Puede volver más tarde para publicar los registros en Route 53 al editar la identidad; consulte the section called “Edición de una identidad mediante la consola”.)

b. Provide DKIM authentication token (BYODKIM) (Proporcionar token de autenticación DKIM [BYODKIM]):

i. Asegúrese de que ya tiene un par de claves públicas y privadas y de que agregó la clave pública a su proveedor de alojamiento DNS. Para obtener más información, consulte the section called “BYODKIM: utilice su propio DKIM”.

ii. En el campo Identity type (Tipo de identidad), elija Provide DKIM authentication token (Proporcionar token de autenticación DKIM).

iii. En Private key (Clave privada), pegue la clave privada que generó desde su par de claves pública y privada. La clave privada debe utilizar al menos el cifrado RSA de 1024 bits y de hasta 2048 bits y debe estar codificada con base64 (PEM).

> **Note**
>
> Debe eliminar la primera y la última línea (`-----BEGIN PRIVATE KEY-----` y `-----END PRIVATE KEY-----`, respectivamente) de la clave privada generada. Además, debe eliminar los saltos de línea en la clave privada generada. El valor resultante es una cadena de caracteres sin espacios ni saltos de línea.

iv. En Selector name (Nombre del selector), ingrese el nombre del selector que debe especificarse en la configuración de DNS de su dominio.

9. Asegúrese de que la casilla de verificación Enabled (Habilitada) esté activada en el campo DKIM signatures (Firmas DKIM).

10. (Opcional) Agregue una o varias Etiquetas a su identidad de dominio. Para ello, incluya una clave de etiqueta y un valor opcional para la clave:

1. Elija Add new tag (Agregar nueva etiqueta) e ingrese la Key (Clave). Puede agregar un valor opcional para la etiqueta.
2. Repita el procedimiento para las etiquetas adicionales sin superar la cantidad de 50, o bien elija Remove (Eliminar) para eliminar etiquetas.

11. Elija Create identity (Crear identidad).

Ahora que se ha creado y configurado la identidad de dominio con DKIM, debe completar el proceso de verificación con el proveedor de DNS; continúe con the section called “Verificación de una identidad de dominio” y siga los procedimientos de autenticación de DNS para el tipo de DKIM con el que configuró la identidad.

Verificación de una identidad de dominio DKIM con el proveedor de DNS

Después de crear la identidad de dominio configurada con DKIM, debe completar el proceso de verificación con su proveedor de DNS mediante los respectivos procedimientos de autenticación para el tipo de DKIM que haya elegido.

Si no ha creado una identidad de dominio, consulte the section called “Creación de una identidad de dominio”.

> **Note**
>
> La verificación de una identidad de dominio requiere acceso a la configuración de DNS del dominio. Los cambios en esta configuración pueden tardar hasta 72 horas en propagarse.

Para verificar la identidad de un dominio DKIM con su proveedor de DNS

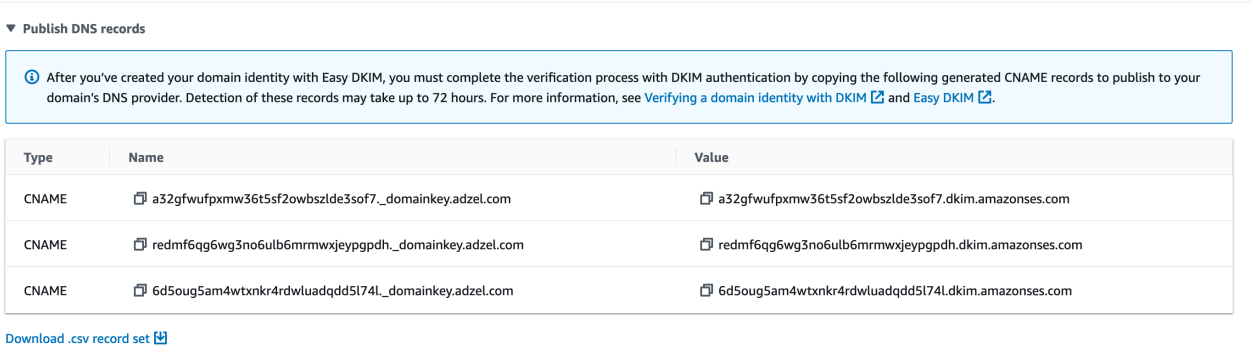
1. En la tabla Loaded identities (Identidades cargadas), seleccione el dominio que desea verificar.
2. En la pestaña Authentication (Autenticación) de la página de detalles de identidad, expanda Publish DNS records (Publicar registros DNS).
3. Según el tipo de DKIM con el que configuró su dominio, Easy DKIM o BYODKIM, siga las instrucciones respectivas:

Easy DKIM

Para verificar un dominio configurado con Easy DKIM

1. Desde la tabla Publish DNS records (Publicar registros DNS), copie los tres registros CNAME que aparecen en esta sección para publicarlos (agregarlos) a su proveedor de DNS. También puede elegir Download .csv record set (Descargar el conjunto de registro .csv) para guardar una copia de los registros en su computadora.

   La siguiente imagen muestra un ejemplo de los registros CNAME a publicar en su proveedor de DNS.



2. Agregue los registros de CNAME a la configuración de DNS de su dominio, correspondiente a su proveedor de alojamiento de DNS:

   - Todos los proveedores de alojamiento de DNS (excluyendo Route 53). Acceda al proveedor de DNS o de alojamiento web de su dominio y agregue los registros CNAME que contienen los valores que copió o guardó anteriormente. Cada proveedor tiene diferentes procedimientos para actualizar los registros de DNS. Consulte la tabla de proveedores de alojamiento y DNS que sigue a estos procedimientos.

     > **Note**
     >
     > Un pequeño número de proveedores de DNS no le permiten incluir guiones bajos (_) en los nombres de registro. Sin embargo, el guion bajo el nombre de registro de DKIM es obligatorio. Si su proveedor de DNS no le permite introducir un guion bajo en el nombre del registro, póngase en contacto con el equipo de atención al cliente del proveedor para obtener ayuda.

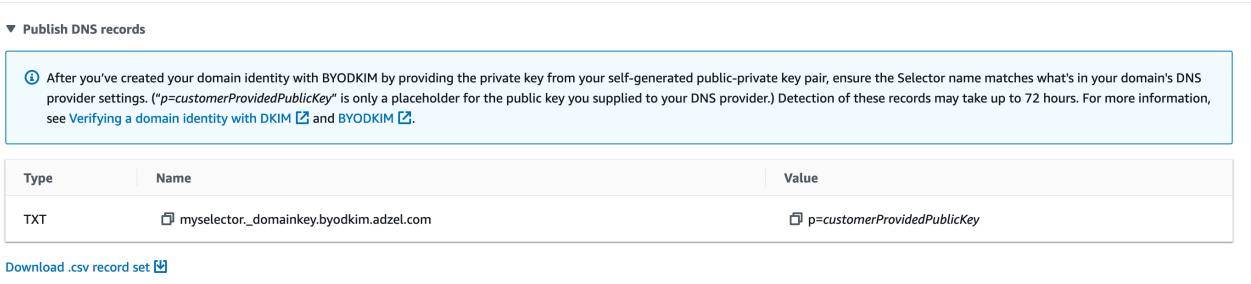
- Route 53 como proveedor de alojamiento de DNS: si utiliza Route 53 en la misma cuenta que utiliza cuando envía correo electrónico mediante SES, y el dominio está registrado, SES actualiza de forma automática la configuración de DNS de su dominio si habilitó SES para publicarla en el momento de la creación. Si no, puede publicarlos fácilmente en Route 53 con un clic en el botón después de la creación. Consulte the section called “Edición de una identidad mediante la consola”. Si la configuración de DNS no se actualiza automáticamente o si desea agregar registros CNAME a Route 53 que no estén en la misma cuenta que utiliza cuando envía correos electrónicos mediante SES, complete los procedimientos que se indican en Edición de registros.
- Si no está seguro de quién es su proveedor de DNS: consulte a su administrador del sistema para obtener más información.

BYODKIM

Para verificar un dominio configurado con BYODKIM

1. Para resumir, cuando creó el dominio con BYODKIM, o configuró u dominio existente con BYODKIM, agregó la clave privada (del par de claves públicas-privadas autogeneradas) y el prefijo del nombre del selector en los campos respectivos de la página Advance DKIM Settings (Configuración avanzada de DKIM) de la consola de SES. Ahora debe completar el proceso de verificación con la actualización de los siguientes registros para su proveedor de alojamiento DNS.
2. En la tabla Publish DNS records (Publicar registros DNS), copie el registro de nombre del selector que aparece en la columna Name (Nombre) para publicarlo (agregarlo) a su proveedor de DNS. También puede elegir Download .csv record set (Descargar el conjunto de registros .csv) para guardar una copia de ellos en su computadora.

   La siguiente imagen muestra un ejemplo del registro de nombre del selector para publicar en su proveedor de DNS.



3. Inicie sesión en el proveedor de DNS o de alojamiento web de su dominio y agregue el registro de nombre del selector que copió o guardó anteriormente. Cada proveedor tiene diferentes procedimientos para actualizar los registros de DNS. Consulte la tabla de proveedores de alojamiento y DNS que sigue a estos procedimientos.

   > **Note**
   >
   > Un pequeño número de proveedores de DNS no le permiten incluir guiones bajos (_) en los nombres de registro. Sin embargo, el guion bajo el nombre de registro de DKIM es obligatorio. Si su proveedor de DNS no le permite introducir un guion bajo en el nombre del registro, póngase en contacto con el equipo de atención al cliente del proveedor para obtener ayuda.

4. Si aún no lo ha hecho, asegúrese de agregar la clave pública del par de claves públicas-privadas autogeneradas a los DNS del dominio o al proveedor de alojamiento web.

   Tenga en cuenta que en la tabla Publish DNS records (Publicar registros DNS), el registro de clave pública que aparece en la columna Value (Valor) solo muestra, “p=customerProvidedPublicKey”, como un marcador de posición para el valor de la clave pública que guardó en el ordenador o que proporcionó a su proveedor de DNS.

   > **Note**
   >
   > Cuando publica (agrega) su clave pública en su proveedor de DNS, debe tener el siguiente formato:
   >
   > - Debe eliminar la primera y la última línea (`-----BEGIN PUBLIC KEY-----` y `-----END PUBLIC KEY-----`, respectivamente) de la clave pública generada. Además, debe eliminar los saltos de línea en la clave pública generada. El valor resultante es una cadena de caracteres sin espacios ni saltos de línea.
   > - Debe incluir en prefijo p= tal y como se muestra en la columna Value (Valor) de la tabla Publish DNS records (Publicar registros DNS).

4. Los cambios en la configuración del DNS pueden tardar hasta 72 horas en propagarse. Tan pronto como Amazon SES detecte todos los registros DKIM requeridos en la configuración DNS de su dominio, el proceso de verificación quedará completado. La configuración de DKIM de su

dominio se mostrará como Successful (Correcta) y Identity status (Estado de identidad) mostrará el valor Verified (Verificado).

5. Si desea configurar y verificar un dominio MAIL FROM personalizado, siga los procedimientos en Configuración del dominio MAIL FROM personalizado.

La tabla que sigue incluye enlaces a la documentación de diversos unos pocos proveedores de DNS muy utilizados. Esta lista no es exhaustiva y no implica aprobación; del mismo modo, si su proveedor de DNS no aparece en la lista, no implica que no pueda usar el dominio con Amazon SES.

Proveedor de DNS/alojamiento	Enlace a la documentación
GoDaddy	Add a CNAME record (enlace externo)
DreamHost	How do I add custom DNS records? (enlace externo)
Cloudflare	Managing DNS records in CloudFlare (enlace externo)
HostGator	Manage DNS Records with HostGator/eNom (enlace externo)
Namecheap	How do I add TXT/SPF/DKIM/DMARC records for my domain? (enlace externo)
Names.co.uk	Changing your domains DNS Settings (enlace externo)
Wix	Adding or Updating CNAME Records in Your Wix Account (enlace externo)

Solución de problemas de verificación de dominios

Si ha realizado los pasos anteriores, pero su dominio no se ha verificado después de 72 horas, verifique lo siguiente:

- Asegúrese de que ha introducido los valores de los registros de DNS en los campos correctos. Algunos proveedores de DNS utilizan nombres distintos para el campo Name/host (Nombre/

anfitrión), como Host (Anfitrión) o Hostname (Nombre de anfitrión). Además, algunos proveedores hacen referencia al campo Record value (Valor de registro) como Points to (Apunta a) o Result (Resultado).

- Asegúrese de que su proveedor no haya adjuntado automáticamente su nombre de dominio en el valor Name/host (Nombre/host) que introdujo en el registro de DNS. Algunos proveedores adjuntan el nombre de dominio sin indicar que lo han hecho. Si el proveedor adjuntó el nombre de dominio al valor Name/host (Nombre/host), elimine el nombre de dominio del final del valor. También puede probar a añadir un punto al final del valor en el registro DNS. Este punto indica al proveedor que el nombre de dominio es un nombre completo.
- El carácter de guion bajo (_) es obligatorio en el valor Name/host (Nombre/host) de cada registro de DNS. Si su proveedor de DNS no permite guiones bajos en los nombres de los registros de DNS, póngase en contacto con el departamento de atención al cliente del proveedor para obtener asistencia adicional.
- Los registros de validación que debe agregar al final de la configuración de DNS del dominio son distintos en cada Región de AWS. Si desea utilizar un dominio para enviar correo electrónico desde varias Regiones de AWS, deberá verificar una identidad de dominio individual en cada una de dichas regiones.

Creación de una identidad de dirección de correo electrónico

Realice el procedimiento siguiente para crear y una identidad de dirección de correo electrónico mediante la consola de Amazon SES.

Para crear una identidad de dirección de correo electrónico (consola)

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).
3. Elija Create identity (Crear identidad).
4. En Identity details (Detalles de la identidad), elija Email address (Dirección de correo electrónico) como el tipo de identidad que desea crear.
5. En Email address (Dirección de correo electrónico), ingrese la dirección de correo electrónico que desea utilizar. La dirección de correo electrónico debe ser una dirección con la que se pueda recibir correo y a la que tenga acceso.

6. (Opcional) Si desea Asignar un conjunto de configuración predeterminado, active la casilla de verificación.

   1. Para Default configuration set (Conjunto de configuración predeterminado), seleccione el conjunto de configuración existente que desee asignar a su identidad. Si aún no ha creado ningún conjunto de configuración, consulte Conjuntos de configuración.

      > **Note**
      >
      > Amazon SES solo toma el conjunto de configuración asignado de manera predeterminada cuando no se especifica ningún otro conjunto en el momento del envío. Si se especifica un conjunto de configuración, Amazon SES aplica el conjunto especificado en lugar del predeterminado.

7. (Opcional) Agregue una o varias Etiquetas a su identidad de dominio. Para ello, incluya una clave de etiqueta y un valor opcional para la clave:

   1. Elija Add new tag (Agregar nueva etiqueta) e ingrese la Key (Clave). Puede agregar un valor opcional para la etiqueta.
   2. Repita el procedimiento para las etiquetas adicionales sin superar la cantidad de 50, o bien elija Remove (Eliminar) para eliminar etiquetas.

8. Para crear la identidad de su dirección de correo electrónico, elija Create identity (Crear identidad). Una vez que se haya creado, debería recibir un correo electrónico de verificación en el plazo de cinco minutos. El siguiente paso es verificar su dirección de correo electrónico. Para ello, siga el procedimiento de verificación que describe en la sección siguiente.

   > **Note**
   >
   > Puede personalizar los mensajes que se envían a las direcciones de correo electrónico que intenta verificar. Para obtener más información, consulte the section called “Uso de plantillas de correo electrónico de verificación personalizado”.

Ahora que ha creado la identidad de la dirección de correo electrónico, debe completar el proceso de verificación; proceda a the section called “Verificación de una identidad de dirección de correo electrónico”.

Verificación de una identidad de dirección de correo electrónico

Después de haber creado la identidad de la dirección de correo electrónico, debe completar el proceso de verificación.

Si no ha creado una identidad de dirección de correo electrónico, consulte the section called “Creación de una identidad de dirección de correo electrónico”.

Para verificar una identidad de dirección de correo electrónico

1. Verifique la bandeja de entrada de la dirección de correo electrónico que utilizó para crear su identidad y busque un correo electrónico de no-reply-aws@amazon.com.
2. Abra el correo electrónico y haga clic en el enlace para completar el proceso de verificación de la dirección de correo electrónico. Una vez que se haya completado el proceso, Identity status (Estado de identidad) se actualizará al valor Verified (Verificado).

Solución de problemas de verificación de direcciones de correo electrónico

Si no recibe el correo electrónico de verificación en un plazo de cinco minutos tras la creación de su identidad, siga los pasos de resolución de problemas que se indican a continuación:

- Asegúrese de que ha ingresado la dirección de correo electrónico correctamente.
- Asegúrese de que la dirección de correo electrónico que ha intentado verificar puede recibir correo electrónico. Puede probarlo mediante otra dirección de correo electrónico para enviar un correo electrónico de prueba a la dirección que desea verificar.
- Consulte su carpeta de correo no deseado.
- El enlace del mensaje de correo electrónico de verificación caduca transcurridas 24 horas. Para enviar un nuevo correo electrónico de verificación, elija la opción Resend (Reenviar) que se encuentra en la parte superior de la página de detalles de la identidad.

Crear y verificar una identidad y asignar un conjunto de configuración predeterminado al mismo tiempo

Puede utilizar la operación CreateEmailIdentity en la API v2 de Amazon SES para crear una nueva identidad de correo electrónico y establecer su configuración predeterminada al mismo tiempo.

> **Note**
>
> Antes de completar el procedimiento de esta sección, primero debe instalar y configurar la AWS CLI. Para obtener más información, consulte la Guía del usuario de AWS Command Line Interface.

Para establecer un conjunto de configuración predeterminado mediante la AWS CLI

- En la línea de comandos, ingrese el siguiente comando para utilizar la operación CreateEmailIdentity.

```
aws sesv2 create-email-identity --email-identity ADDRESS-OR-DOMAIN --configuration-set-name CONFIG-SET
```

En los comandos anteriores, sustituya *ADDRESS-OR-DOMAIN* con la identidad del correo electrónico que desea verificar. Reemplace *CONFIG-SET* con el nombre del conjunto de configuración que desea establecer como conjunto de configuración predeterminado para la identidad.

Si el comando se ejecuta correctamente, termina sin proporcionar ninguna salida.

To verify your email address (Para verificar su dirección de correo electrónico)

1. Compruebe la bandeja de entrada de la dirección de correo electrónico que está verificando. Recibirá un mensaje con una línea de asunto similar a la siguiente: “Amazon Web Services - Email Address Verification Request in region *RegionName*” (Amazon Web Services: Solicitud de verificación de dirección de email en la región RegionName), donde *RegionName* es el nombre de la región de Región de AWS en la que intentó verificar la dirección de correo electrónico.

   Abra el mensaje y, a continuación, haga clic en el enlace que contiene.

   > **Note**
   >
   > El enlace del mensaje de verificación caduca 24 horas después de su envío. Si han transcurrido más de 24 horas desde que recibió el correo electrónico de verificación, repita los pasos 1 a 5 para recibir un correo electrónico de verificación con un enlace válido.

2. En la consola de Amazon SES, en Identity Management (Administración de identidad), elija Email Addresses (Direcciones de email). En la lista de direcciones de correo electrónico, localice la

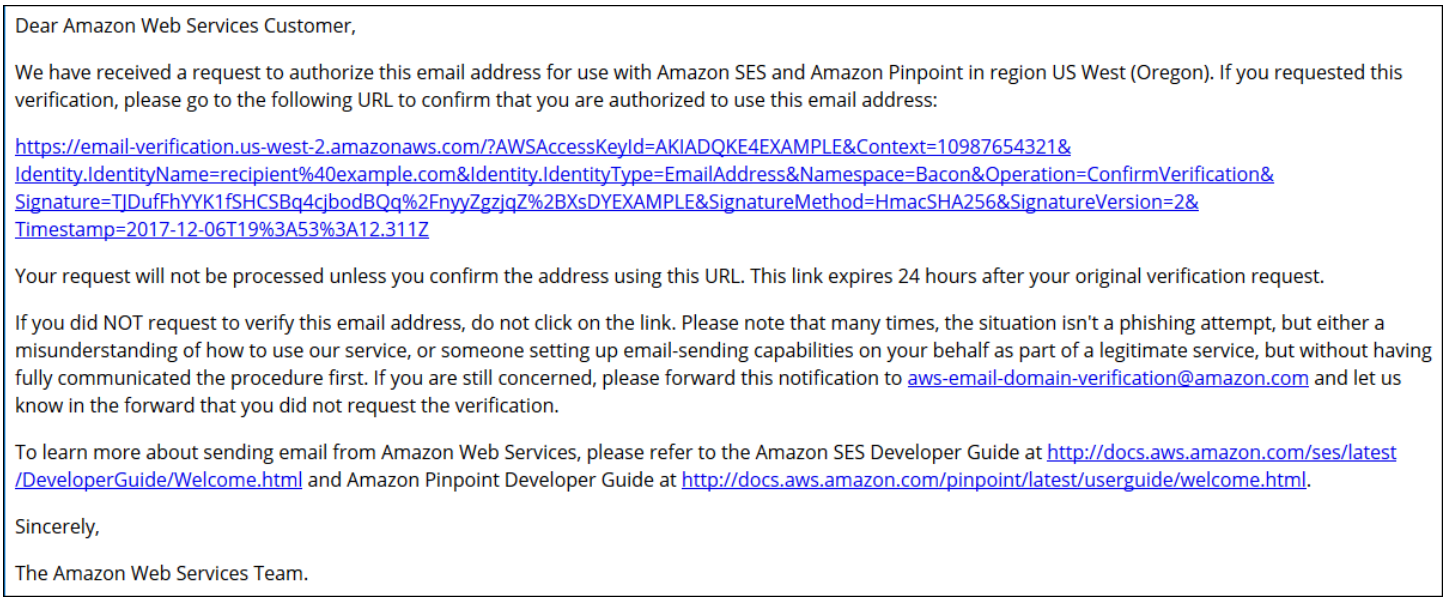
dirección de correo electrónico que está verificando. Si la dirección de correo electrónico está verificada, el valor de la columna Status es "verified".

To verify your domain (Para verificar su dominio)

Si ha ingresado un nombre de dominio para el parámetro `--email-identity` en el procedimiento de línea de comandos anterior, consulte Verificación de una identidad de dominio para obtener más información.

Uso de plantillas de correo electrónico de verificación personalizado

Cuando intenta verificar una dirección de correo electrónico, Amazon SES envía un correo electrónico a una dirección similar a la del ejemplo que se muestra en la siguiente imagen.



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=109876543210&Identity.IdentityName=recipient%40example.com&Identity.IdentityType=EmailAddress&Namespace=Bacon&Operation=ConfirmVerification&Signature=TJDufFhYYK1fSHCSBq4cjbodBQq%2FnyyZgzjqZ%2BXsDYEXAMPLE&SignatureMethod=HmacSHA256&SignatureVersion=2&Timestamp=2017-12-06T19%3A53%3A12.311Z

Your request will not be processed unless you confirm the address using this URL. This link expires 24 hours after your original verification request.

If you did NOT request to verify this email address, do not click on the link. Please note that many times, the situation isn't a phishing attempt, but either a misunderstanding of how to use our service, or someone setting up email-sending capabilities on your behalf as part of a legitimate service, but without having fully communicated the procedure first. If you are still concerned, please forward this notification to aws-email-domain-verification@amazon.com and let us know in the forward that you did not request the verification.

To learn more about sending email from Amazon Web Services, please refer to the Amazon SES Developer Guide at http://docs.aws.amazon.com/ses/latest/DeveloperGuide/Welcome.html and Amazon Pinpoint Developer Guide at http://docs.aws.amazon.com/pinpoint/latest/userguide/welcome.html.

Sincerely,

The Amazon Web Services Team.

Varios clientes de Amazon SES crean aplicaciones (como conjuntos de aplicaciones de marketing por correo electrónico o sistemas de tramitación de incidencias) que envían correo electrónico por medio de Amazon SES en nombre de sus propios clientes. Para los usuarios finales de estas aplicaciones, el proceso de verificación del correo electrónico puede ser confuso: el correo electrónico de verificación utiliza la información de marca de Amazon SES, en lugar de la información de marca de la aplicación, y los usuarios finales nunca se han registrado para utilizar Amazon SES directamente.

Si su caso de uso de Amazon SES requiere que las direcciones de correo electrónico de los clientes se verifiquen para poder usarlas con Amazon SES, puede crear mensajes de correo electrónico de verificación personalizados. Estos mensajes de correo electrónico personalizados ayudan a reducir

la confusión de los clientes y aumentan la velocidad a las que sus clientes realizan el proceso de registro.

> **Note**
>
> Para utilizar esta característica, su cuenta de Amazon SES tiene que estar fuera del entorno de pruebas. Para obtener más información, consulte Solicitar acceso a la producción (salir del entorno de pruebas de Amazon SES).

Temas de esta sección:

- Creación de una plantilla de correo electrónico de verificación personalizado
- Edición de una plantilla de correo electrónico de verificación personalizado
- Envío de correos electrónicos de verificación usando plantillas personalizadas
- Preguntas frecuentes sobre el correo electrónico de verificación personalizado

Creación de una plantilla de correo electrónico de verificación personalizado

Para crear un mensaje de correo electrónico de verificación personalizado, use la operación de la API `CreateCustomVerificationEmailTemplate`. Esta operación toma los siguientes parámetros de entrada:

Atributo	Descripción
`TemplateName`	El nombre de la plantilla. El nombre que especifique debe ser único.
`FromEmailAddress`	La dirección de correo electrónico desde la que se envía el correo electrónico de verificación. La dirección o el dominio que especifique deben verificarse para su uso con su cuenta de Amazon SES. **Note** El atributo `FromEmailAddress` no admite nombres de visualización (también conocidos como nombres de "remitente descriptivo").

Atributo	Descripción
`TemplateSubject`	La línea de asunto del correo electrónico de verificación.
`TemplateContent`	El cuerpo del mensaje de correo electrónico. El cuerpo del mensaje de correo electrónico pueden contener HTML, con algunas restricci ones. Para obtener más información, consulte Preguntas frecuentes sobre el correo electrónico de verificación personalizado.
`SuccessRedirection URL`	La dirección URL a la que se envía a los usuarios si sus direcciones de correo electrónico se verifican correctamente.
`FailureRedirection URL`	La dirección URL a la que se envía a los usuarios si sus direcciones de correo electrónico no se verifican correctamente.

Puede utilizar los SDK de AWS o la AWS CLI para crear una plantilla de correo electrónico de verificación personalizado con la operación `CreateCustomVerificationEmailTemplate`. Para obtener más información acerca de los SDK de AWS, consulte Herramientas para Amazon Web Services. Para obtener más información sobre la AWS CLI, consulte Interfaz de línea de comandos de AWS.

La siguiente sección incluye procedimientos para crear un correo electrónico de verificación personalizado mediante la AWS CLI. Para estos procedimientos se presupone que ha instalado y configurado la AWS CLI. Para obtener más información sobre cómo instalar y configurar la AWS CLI, consulte la Guía del usuario de la AWS Command Line Interface.

> **Note**
>
> Para completar el procedimiento de esta sección, debe utilizar la versión 1.14.6 o posterior de la AWS CLI. Para obtener mejores resultados, actualice a la última versión de la AWS CLI. Para obtener información acerca de la instalación o actualización de la AWS CLI, consulte Instalación de la AWS Command Line Interface en la Guía del usuario de la AWS Command Line Interface.

1. En un editor de texto, cree un nuevo archivo. Pegue el siguiente contenido en el editor:

```
{
```

```
  "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**
>
> Para que el ejemplo anterior sea más fácil de leer, el atributo `TemplateContent` contiene saltos de línea. Si pega el ejemplo anterior en el archivo de texto, elimine los saltos de línea antes de continuar.

Reemplace los valores de `TemplateName`, `FromEmailAddress`, `TemplateSubject`, `TemplateContent`, `SuccessRedirectionURL` y `FailureRedirectionURL` por sus propios valores.

> **Note**
>
> La dirección de correo electrónico que especifique para el parámetro `FromEmailAddress` tiene que estar verificada o tiene que ser una dirección en un dominio verificado. Para obtener más información, consulte Identidades verificadas en Amazon SES.

Cuando haya terminado, guarde el archivo como `customverificationemail.json`.

2. En la línea de comandos, escriba el siguiente comando para crear la plantilla de correo electrónico de verificación personalizado:

```
aws sesv2 create-custom-verification-email-template --cli-input-json file://
customverificationemail.json
```

3. (Opcional) Puede confirmar que la plantilla se ha creado escribiendo el comando siguiente:

```
aws sesv2 list-custom-verification-email-templates
```

Edición de una plantilla de correo electrónico de verificación personalizado

Puede editar una plantilla de correo electrónico de verificación personalizado mediante la operación `UpdateCustomVerificationEmailTemplate`. Esta operación acepta los mismos parámetros de entrada que la operación `CreateCustomVerificationEmailTemplate` (es decir, los atributos `TemplateName`, `FromEmailAddress`, `TemplateSubject`, `TemplateContent`, `SuccessRedirectionURL` y `FailureRedirectionURL`). Sin embargo, con la operación `UpdateCustomVerificationEmailTemplate`, ninguno de estos atributos son obligatorios. Cuando pasa un valor para `TemplateName` que es igual al nombre de una plantilla de correo electrónico de verificación personalizado, los atributos que especifique sobrescriben los que se encuentran originalmente en la plantilla.

Envío de correos electrónicos de verificación usando plantillas personalizadas

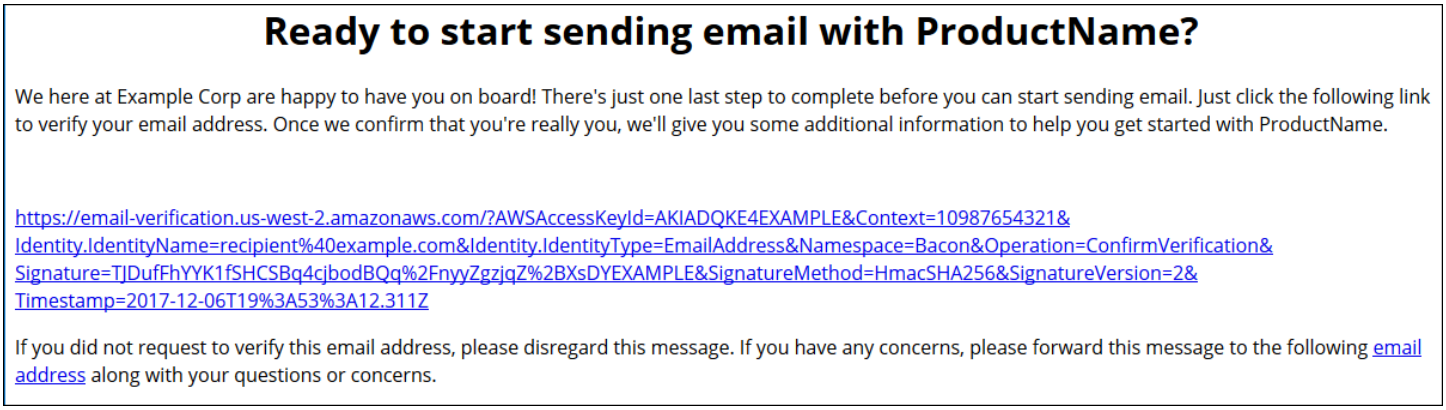
Después de crear al menos una plantilla de correo electrónico de verificación personalizado, puede enviarla a sus clientes llamando a la operación de la API SendCustomVerificationEmail. Puede llamar a la operación `SendCustomVerificationEmail` mediante cualquiera de los SDK de AWS o la AWS CLI. La operación `SendCustomVerificationEmail` toma los siguientes parámetros de entrada:

Atributo	Descripción
`EmailAddress`	La dirección de correo electrónico que se va a verificar.
`TemplateName`	El nombre de la plantilla de correo electrónico de verificación personalizado que se envía a la dirección de correo electrónico que va a verificar.

Atributo	Descripción
`ConfigurationSetName`	(Opcional) El nombre del conjunto de configuración que se va a usar al enviar el correo electrónico de verificación.

Suponga, por ejemplo, que sus clientes se registran en el servicio mediante un formulario de su aplicación. Cuando el cliente completa el formulario y lo envía, su aplicación llama a la operación `SendCustomVerificationEmail`, pasando la dirección de correo electrónico del cliente y el nombre de la plantilla que desee utilizar.

El cliente recibe un correo electrónico que utiliza la plantilla de correo electrónico personalizado que ha creado. Amazon SES agrega automáticamente un enlace único para el destinatario, así como una breve renuncia de responsabilidades. En la siguiente imagen se muestra un correo electrónico de verificación de ejemplo que utiliza la plantilla creada en Creación de una plantilla de correo electrónico de verificación personalizado.



Ready to start sending email with ProductName?

We here at Example Corp are happy to have you on board! There's just one last step to complete before you can start sending email. Just click the following link to verify your email address. Once we confirm that you're really you, we'll give you some additional information to help you get started with ProductName.

https://email-verification.us-west-2.amazonaws.com/?AWSAccessKeyId=AKIADQKE4EXAMPLE&Context=10987654321&Identity.IdentityName=recipient%40example.com&Identity.IdentityType=EmailAddress&Namespace=Bacon&Operation=ConfirmVerification&Signature=TJDufFhYYK1fSHCSBq4cjbodBQq%2FnyyZgzjqZ%2BXsDYEXAMPLE&SignatureMethod=HmacSHA256&SignatureVersion=2&Timestamp=2017-12-06T19%3A53%3A12.311Z

If you did not request to verify this email address, please disregard this message. If you have any concerns, please forward this message to the following email address along with your questions or concerns.

Preguntas frecuentes sobre el correo electrónico de verificación personalizado

Esta sección contiene respuestas a preguntas frecuentes acerca de la característica de plantilla de correo electrónico de verificación personalizado.

Q1 (P1). ¿Cuántas plantillas de correo electrónico de verificación personalizado puedo crear?

Puede crear hasta 50 plantillas de correo electrónico de verificación personalizado para cada cuenta de Amazon SES.

Q2 (P2). ¿Cómo se muestran los mensajes de correo electrónico de verificación personalizados a los destinatarios?

Los mensajes de correo electrónico de verificación personalizados incluyen el contenido que especificó al crear la plantilla, seguido de un enlace en el que los destinatarios deben hacer clic para verificar sus direcciones de correo electrónico.

Q3 (P3). ¿Puedo obtener una vista previa del correo electrónico de verificación personalizado?

Para obtener una vista previa de un correo electrónico de verificación personalizado, utilice la operación `SendCustomVerificationEmail` para enviar un correo electrónico de verificación a una dirección de su propiedad. Si no hace clic en el enlace de verificación, Amazon SES no creará ninguna identidad nueva. Si hace clic en el enlace de verificación, podrá eliminar la identidad recién creada mediante la operación `DeleteIdentity`.

P4. ¿Puedo incluir imágenes en mis plantillas de correo electrónico de verificación personalizado?

Puede incrustar imágenes en el código HTML para las plantillas a través de la codificación Base64. Cuando incrusta imágenes de esta forma, Amazon SES las convierte automáticamente en archivos adjuntos. Puede codificar una imagen en la línea de comandos ejecutando uno de los siguientes comandos:

Linux, macOS, or Unix

```
base64 -i imagefile.png | tr -d '\n' > output.txt
```

Windows

```
certutil -encodehex -f imagefile.png output.txt 0x40000001
```

Reemplace *`imagefile.png`* por el nombre del archivo que desea codificar. En ambos de los comandos anteriores, la imagen codificada en Base64 se almacena en `output.txt`.

Puede incrustar la imagen codificada en Base64 incluyendo lo siguiente en el código HTML de la plantilla: `<img src="`*`base64EncodedImage`*`"/>`

En el ejemplo anterior, sustituya *`png`* por el tipo de archivo de la imagen codificada (por ejemplo, jpg o gif) y sustituya *`base64EncodedImage`* por la imagen codificada en base64 (es decir, el contenido de `output.txt` de uno de los comandos anteriores).

P5. ¿Existe algún límite en el contenido que puedo incluir en las plantillas de correo electrónico de verificación personalizado?

Las plantillas de correo electrónico de verificación personalizado no pueden tener más de 10 MB. Además, las plantillas de correo electrónico de verificación personalizado que contienen HTML solo pueden utilizar las etiquetas y atributos que se muestran en la siguiente tabla.

Etiqueta HTML	Atributos permitidos
abbr	class, id, style, title
acronym	class, id, style, title
address	class, id, style, title
area	class, id, style, title
b	class, id, style, title
bdo	class, id, style, title
big	class, id, style, title
blockquote	cite, class, id, style, title
body	class, id, style, title
br	class, id, style, title
button	class, id, style, title
caption	class, id, style, title
center	class, id, style, title
cite	class, id, style, title
code	class, id, style, title
col	class, id, span, style, title, width

Etiqueta HTML	Atributos permitidos
colgroup	class, id, span, style, title, width
dd	class, id, style, title
del	class, id, style, title
dfn	class, id, style, title
dir	class, id, style, title
div	class, id, style, title
dl	class, id, style, title
dt	class, id, style, title
em	class, id, style, title
fieldset	class, id, style, title
font	class, id, style, title
form	class, id, style, title
h1	class, id, style, title
h2	class, id, style, title
h3	class, id, style, title
h4	class, id, style, title
h5	class, id, style, title
h6	class, id, style, title
head	class, id, style, title
hr	class, id, style, title

Etiqueta HTML	Atributos permitidos
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
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

Etiqueta HTML	Atributos permitidos
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
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

Etiqueta HTML	Atributos permitidos
`var`	`class, id, style, title`

> **Note**
>
> Las plantillas de correo electrónico de verificación personalizado no pueden incluir etiquetas de comentario.

P6. ¿Cuántas direcciones de correo electrónico verificadas pueden existir en mi cuenta?

Su cuenta de Amazon SES puede tener hasta 10 000 identidades verificadas en cada región de AWS. En Amazon SES, las identidades incluyen dominios y direcciones de correo electrónico verificados.

P7. ¿Puedo crear plantillas de correo electrónico de verificación personalizado mediante la consola de Amazon SES?

Actualmente, solo es posible crear, editar y eliminar los mensajes de correo electrónico de verificación personalizados mediante la API de Amazon SES.

P8. ¿Puedo realizar un seguimiento de los eventos "open" y "click" que se producen cuando los clientes reciben mensajes de correo electrónico de verificación personalizados?

Los mensajes de correo electrónico de verificación personalizados no pueden incluir un seguimiento de los eventos de apertura o clics.

P9. ¿Pueden los mensajes de correo electrónico de verificación personalizados incluir encabezados personalizados?

Los mensajes de correo electrónico de verificación personalizados no pueden incluir encabezados personalizados.

P10. ¿Puedo eliminar el texto que aparece en la parte inferior de los mensajes de correo electrónico de verificación personalizados?

El siguiente texto se agrega automáticamente al final de cada mensaje de correo electrónico de verificación personalizado y no se puede eliminar:

Si no solicitó verificar esta dirección de correo electrónico, descarte este mensaje.

P11. ¿Están los mensajes de correo electrónico de verificación personalizados firmados con DKIM?

Para que los mensajes de correo electrónico de verificación se firmen con DKIM, la dirección de correo electrónico que especifique en el atributo `FromEmailAddress` al crear la plantilla de correo electrónico de verificación debe configurarse para generar una firma DKIM. Para obtener más información sobre cómo configurar DKIM para los dominios y direcciones de correo electrónico, consulte the section called “Autenticación de correo electrónico con DKIM”.

P12. ¿Por qué no aparecen las operaciones de la API de la plantilla de correo electrónico de verificación personalizada en el SDK o en la CLI?

Si no puede utilizar las operaciones de la plantilla de correo electrónico de verificación personalizada en una SDK o en la AWS CLI, es posible que esté utilizando una versión más antigua del SDK o de la CLI. Las operaciones de la plantilla de correo electrónico de verificación personalizada están disponibles en los siguientes SDK y CLI:

- Versión 1.14.6 o posterior de la AWS Command Line Interface
- Versión 3.3.205.0 o posterior del AWS SDK for .NET
- Versión 1.3.20170531.19 o posterior del AWS SDK para C++
- Versión 1.12.43 o posterior del AWS SDK for Go
- Versión 1.11.245 o posterior del AWS SDK for Java
- Versión 2.166.0 o posterior del AWS SDK for JavaScript
- Versión 3.45.2 o posterior del AWS SDK for PHP
- Versión 1.5.1 o posterior del AWS SDK for Python (Boto)
- Versión 1.5.0 o posterior de la gema `aws-sdk-ses` en el AWS SDK for Ruby

P13. ¿Por qué recibo errores **`ProductionAccessNotGranted`** cuando envío correos electrónicos de verificación personalizados?

El error `ProductionAccessNotGranted` indica que su cuenta sigue estando en el entorno de pruebas de Amazon SES. Solo puede enviar correos electrónicos de verificación personalizados si su cuenta se ha eliminado del entorno de pruebas. Para obtener más información, consulte Solicitar acceso a la producción (salir del entorno de pruebas de Amazon SES).

Administración de identidades en Amazon SES

En la consola de Amazon SES, puede ver una lista de identidades, abrir una identidad para ver y editar su configuración, asociar una configuración predeterminada o eliminar una o varias identidades.

> **Note**
>
> Los procedimientos descritos en esta sección se aplican solo a las identidades de la Región de AWS seleccionada. Para administrar identidades que se crearon en más de una región, repita los procedimientos para cada Región de AWS.

Visualización de una lista de identidades en Amazon SES

Puede utilizar la consola o la API de Amazon SES para ver una lista de las identidades de dominios y direcciones de correo electrónico verificadas o pendientes de verificación. También puede ver las identidades cuya verificación no se completó correctamente.

Para ver las identidades de su dominio y dirección de correo electrónico (consola)

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En la consola, utilice el selector de regiones para elegir la Región de AWS para la que desea ver su lista de identidades.

   > **Note**
   >
   > Este procedimiento solo muestra una lista de identidades para la Región de AWS seleccionada.

3. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas). La tabla Loaded identities (Identidades cargadas) muestra tanto las identidades de dominio como de dirección de correo electrónico. La columna Status (Estado) muestra si una identidad se ha verificado, si está pendiente de verificación o si el proceso de verificación no se completó correctamente. Las definiciones de todos los valores posibles de estado son las siguientes:

- Verified (Verificado): su identidad se ha verificado correctamente para realizar envíos en SES.
- Failure (Error): SES no ha podido verificar su identidad. Si se trata de un dominio, significa que SES no pudo detectar los registros de DNS en las últimas 72 horas. Si se trata de una dirección de correo electrónico, significa que el correo electrónico de verificación que se envió a la dirección de correo electrónico no se ha confirmado en un plazo de 24 horas.
- Pending (Pendiente): SES sigue intentando verificar la identidad.
- Temporary Failure (Error temporal): en el caso de un dominio verificado previamente, SES comprobará de forma periódica el registro de DNS necesario para la verificación. Si en algún momento SES no puede detectar el registro, el estado cambia a Temporary Failure (Error temporal). SES volverá a comprobar el registro de DNS durante 72 horas y, si no puede detectarlo, el estado del dominio cambia a Failure (Error). Si puede se detectar el registro, el estado del dominio cambia a Verified (Verificado).
- Not started (No iniciado): aún no ha iniciado el proceso de verificación.

4. Para ordenar las identidades por estado de verificación, elija la columna Status (Estado).
5. Para ver la página de detalles de una identidad, seleccione la identidad que desea ver.

Eliminación de una identidad en Amazon SES

Puede utilizar la consola o la API de Amazon SES para eliminar una identidad de dominio o dirección de correo electrónico de su cuenta en la Región de AWS seleccionada.

Para eliminar una identidad de dominio o dirección de correo electrónico (consola)

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En la consola, utilice el selector de regiones para elegir la Región de AWS de la que desea eliminar una o varias identidades.
3. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).

   La tabla Loaded identities (Identidades cargadas) muestra una lista tanto las identidades de dominio como de dirección de correo electrónico.
4. En la columna Identity (Identidad), seleccione la identidad que desea eliminar. Es posible eliminar varias identidades. Para ello, active la casilla situada junto a cada identidad que desee eliminar.

5. Elija Delete (Eliminar).

Edición de una identidad existente en Amazon SES

Puede utilizar la consola o la API de Amazon SES para editar una identidad de dominio o dirección de correo electrónico de su cuenta en la Región de AWS seleccionada.

Para editar una identidad de dominio o dirección de correo electrónico (consola)

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En la consola, utilice el selector de regiones para elegir la Región de AWS de la que desea editar una o varias identidades.
3. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).

   La tabla Loaded identities (Identidades cargadas) muestra una lista tanto las identidades de dominio como de dirección de correo electrónico.
4. En la columna Identity (Identidad), seleccione la identidad que desea editar (al hacer clic directamente en el nombre de la identidad en lugar de seleccionar su casilla de verificación).
5. En la página de detalles de la identidad, seleccione la pestaña que contiene las categorías que quiere editar.
6. En cualquiera de los contenedores categóricos de la pestaña seleccionada, elija el botón Edit (Editar) del atributo que desea editar, haga los cambios y, a continuación, elija Save changes (Guardar los cambios).

   a. Si desea editar atributos desde la pestaña Authentication (Autenticación) y su identidad de dominio está alojada en Amazon Route 53, y aún no ha publicado sus registros de DNS, habrá un botón Publish DNS records to Route53 (Publicar registros de DNS en Route 53) (junto al botón Edit [Editar]) en uno de los DomainKeys Identified Mail (DKIM) [Correo identificado con claves de dominio (DKIM)] o Custom MAIL FROM domain(Dominio MAIL FROM personalizado), o en ambos.

> **Note**
>
> La pestaña Authentication (Autenticación) solo está presente cuando su cuenta tiene un dominio verificado o una dirección de correo electrónico que utiliza un dominio verificado en su cuenta.

b. Puede publicar los registros DNS directamente desde el botón Publish DNS records to Route 53 (Publicar registros DNS en Route 53): simplemente haga clic en él, se mostrará un banner de confirmación y el botón Publish DNS records to Route 53 (Publicar registros DNS en Route 53) ya no estará visible para el contenedor correspondiente.

7. Repita los pasos 5 y 6 para cada atributo de la identidad que quiera editar.

Editar una identidad para utilizar un conjunto de configuración predeterminado mediante la API

Puede utilizar la operación PutEmailIdentityConfigurationSetAttributes para agregar o quitar un conjunto de configuración predeterminado de una identidad de correo electrónico existente.

> **Note**
>
> Antes de completar el procedimiento de esta sección, primero debe instalar y configurar la AWS CLI. Para obtener más información, consulte la Guía del usuario de AWS Command Line Interface.

Para agregar un conjunto de configuración predeterminada mediante la AWS CLI

- En la línea de comandos, escriba el comando siguiente para utilizar la operación PutEmailIdentityConfigurationSetAttributes.

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

En los comandos anteriores, sustituya *ADDRESS-OR-DOMAIN* con la identidad del correo electrónico que desea verificar. Reemplace *CONFIG-SET* con el nombre del conjunto de configuración que desea establecer como conjunto de configuración predeterminado para la identidad.

Si el comando se ejecuta correctamente, termina sin proporcionar ninguna salida.

Para eliminar un conjunto de configuración predeterminada mediante la AWS CLI

- En la línea de comandos, escriba el comando siguiente para utilizar la operación PutEmailIdentityConfigurationSetAttributes.

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

En los comandos anteriores, sustituya *ADDRESS-OR-DOMAIN* con la identidad del correo electrónico que desea verificar.

Si el comando se ejecuta correctamente, termina sin proporcionar ninguna salida.

Recuperar el conjunto de configuración predeterminado utilizado por la identidad (API)

Puede utilizar la operación GetEmailIdentity para recuperar el conjunto de configuración predeterminado para una identidad de correo electrónico, si corresponde.

> **Note**
>
> Antes de completar el procedimiento de esta sección, primero debe instalar y configurar la AWS CLI. Para obtener más información, consulte la Guía del usuario de AWS Command Line Interface.

Para recuperar un conjunto de configuración predeterminado mediante la AWS CLI

- En la línea de comandos, ingrese el siguiente comando para utilizar la operación GetEmailIdentity.

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

En los comandos anteriores, reemplace *ADDRESS-OR-DOMAIN* con la identidad de correo electrónico para la que desea conocer el conjunto de configuración predeterminado, si lo hubiera.

Si el comando se ejecuta correctamente, proporciona a un objeto JSON los detalles de identidad de correo electrónico.

Anular el conjunto de configuración predeterminado utilizado por la identidad (API)

Puede utilizar la operación SendEmail para enviar correo electrónico con un conjunto de configuración diferente. Si lo hace, el conjunto de configuración que especifique anula el conjunto de configuración predeterminado de la identidad.

> **Note**
>
> Antes de completar el procedimiento de esta sección, primero debe instalar y configurar la AWS CLI. Para obtener más información, consulte la Guía del usuario de AWS Command Line Interface.

Para invalidar un conjunto de configuración predeterminado mediante la AWS CLI

- En la línea de comandos, ingrese el siguiente comando para utilizar la operación SendEmail.

```
aws sesv2 send-email --destination file://DESTINATION-JSON --content file://CONTENT-JSON --from-email-address ADDRESS-OR-DOMAIN --configuration-set-name CONFIG-SET
```

En los comandos anteriores, reemplace *DESTINATION-JSON* con su archivo JSON de destino, *CONTENT-JSON* con su archivo JSON de contenido, *ADDRESS-OR-DOMAIN* con su dirección de correo electrónico FROM y *CONFIG-SET* con el nombre del conjunto de configuración que desea utilizar en lugar del conjunto de configuración predeterminado para la identidad.

Si el comando se ejecuta correctamente, genera un `MessageId`.

Configuración de identidades en Amazon SES

Amazon Simple Email Service (Amazon SES) utiliza el Simple Mail Transfer Protocol (SMTP) para enviar correo electrónico. Dado que SMTP no ofrece por sí solo ninguna autenticación, los spammers pueden enviar mensajes de correo electrónico que afirmen proceder de otra persona, ocultando así su verdadero origen. Mediante la falsificación de encabezados de correo electrónico

y la suplantación de direcciones IP de origen, los spammers pueden engañar a los destinatarios diciéndoles que los mensajes de correo electrónico que están recibiendo son auténticos.

La mayoría de los ISP que reenvían tráfico de correo electrónico adoptan medidas a fin de evaluar si el correo electrónico es legítimo. Una de las medidas que adoptan los ISP consiste en determinar si un correo electrónico está autenticado. La autenticación requiere que los remitentes verifiquen que son el propietario de la cuenta desde la que están enviando el correo. En algunos casos, los ISP rechazan reenviar el correo electrónico que no está autenticado. Para garantizar una capacidad de entrega óptima, le recomendamos que autentique su correo electrónico.

En las siguientes secciones, se describen dos mecanismos de autenticación que utilizan los ISP, el marco de políticas de remitentes (SPF) y DomainKeys Identified Mail (DKIM), asimismo se ofrecen instrucciones sobre cómo usar estos estándares con Amazon SES.

- Para obtener más información acerca de SPF, que proporciona una forma de rastrear un mensaje de correo electrónico hasta el sistema desde el que se envió, consulte Autenticación de correo electrónico con SPF en Amazon SES.
- Para obtener más información acerca de DKIM, una norma que le permite firmar los mensajes de correo electrónico para mostrar a los ISP que sus mensajes son legítimos y no han sido modificados en tránsito, consulte Autenticación de correo electrónico con DKIM en Amazon SES.
- Para obtener información sobre cómo cumplir con Domain-based Message Authentication, Reporting and Conformance (DMARC), que se basa en SPF y DKIM, consulte Cumplimiento del protocolo de autenticación DMARC en Amazon SES.

Métodos de autenticación del correo electrónico

Amazon Simple Email Service (Amazon SES) utiliza el Simple Mail Transfer Protocol (SMTP) para enviar correo electrónico. Dado que SMTP no ofrece por sí solo ninguna autenticación, los spammers pueden enviar mensajes de correo electrónico que declaren proceder de otra persona, ocultando así su verdadero origen. Mediante la falsificación de encabezados de correo electrónico y la suplantación de direcciones IP de origen, los spammers pueden engañar a los destinatarios diciéndoles que los mensajes de correo electrónico que están recibiendo son auténticos.

La mayoría de los ISP que reenvían tráfico de correo electrónico adoptan medidas a fin de evaluar si el correo electrónico es legítimo. Una de las medidas que adoptan los ISP consiste en determinar si un correo electrónico está autenticado. La autenticación requiere que los remitentes verifiquen que son el propietario de la cuenta desde la que están enviando el correo. En algunos casos, los ISP

rechazan reenviar el correo electrónico que no está autenticado. Para garantizar una capacidad de entrega óptima, le recomendamos que autentique su correo electrónico.

Contenido

- Autenticación de correo electrónico con DKIM en Amazon SES
- Autenticación de correo electrónico con SPF en Amazon SES
- Uso de un dominio MAIL FROM personalizado
- Cumplimiento del protocolo de autenticación DMARC en Amazon SES
- Uso de BIMI en Amazon SES

Autenticación de correo electrónico con DKIM en Amazon SES

DomainKeys Identified Mail (DKIM) es un estándar de seguridad de correo electrónico diseñado para asegurarse de que un correo electrónico que supuestamente procede de un dominio específico haya sido autorizado por el propietario de dicho dominio. Este estándar utiliza criptografía de clave pública para firmar un correo electrónico con una clave privada. Los servidores destinatarios pueden utilizar una clave pública publicada en el DNS de un dominio para verificar que partes del correo electrónico no se hayan modificado durante el tránsito.

Las firmas DKIM son opcionales. Puede decidir firmar sus correos electrónicos con una firma DKIM para mejorar la capacidad de entrega con proveedores de correo electrónico conformes con DKIM. Amazon SES le ofrece dos opciones para firmar sus mensajes con una firma DKIM:

- Easy DKIM: SES genera un par de claves pública-privada y agrega automáticamente una firma de DKIM a cada mensaje que envíe desde dicha identidad, consulte Easy DKIM en Amazon SES.
- BYODKIM (Utilice su propio DKIM): puede proporcionar su propio par de claves pública-privada y SES agrega una firma de DKIM a cada mensaje que envíe desde dicha identidad, consulte Uso de su propio token de autenticación (BYODKIM) de DKIM en Amazon SES.
- Agregar manualmente una firma de DKIM: puede agregar la firma de DKIM propia al correo electrónico que envíe con la API `SendRawEmail`, consulte Firma DKIM manual en Amazon SES.

Longitud de clave de firma de DKIM

Dado que muchos proveedores de DNS ahora admiten totalmente el cifrado RSA DKIM de 2048 bits, Amazon SES también admite DKIM 2048 para permitir una autenticación más segura de los correos electrónicos y, por lo tanto, la utiliza como longitud de clave predeterminada al configurar Easy DKIM

desde la API o la consola. También puede configurar y utilizar las claves de 2048 bits con el método de uso de su propio DKIM (BYODKIM), donde la longitud de la clave de firma debe ser de al menos 1024 bits y no superior a 2048 bits.

Por razones de seguridad capacidad de entrega del correo electrónico, cuando se configura con Easy DKIM, podrá utilizar las longitudes de clave de 1024 y 2048 bits junto y dispondrá de flexibilidad para volver a utilizar la longitud de 1024 bits en caso de problemas con cualquier proveedor de DNS que todavía no admita la longitud de 2048 bits. Cuando cree una nueva identidad, esta se creará con DKIM 2048 de forma predeterminada, a menos que especifique la longitud de 1024 bits.

Para preservar la capacidad de entrega del correo electrónico en tránsito, existen restricciones sobre la frecuencia con la que puede cambiar la longitud de la clave DKIM. Entre las restricciones se incluyen las siguientes:

- No se puede cambiar a la misma longitud de clave que ya está configurada.
- No se puede cambiar a una longitud de clave diferente más de una vez en un período de 24 horas (a menos que sea la primera actualización a 1024 en dicho período).

Cuando el correo electrónico está en tránsito, el DNS utiliza su clave pública para autenticar el correo electrónico; por lo tanto, si cambia las claves con demasiada rapidez o frecuencia, es posible que el DNS no pueda autenticar con DKIM el correo electrónico, ya que es posible que la clave anterior ya esté invalidada. Estas restricciones evitan este problema.

Consideraciones de DKIM

Cuando se utiliza DKIM para autenticar el correo electrónico, se aplican las reglas siguientes:

- Solo tiene que configurar DKIM para el dominio que utiliza en la dirección “From” (Remitente). No es necesario que configure DKIM para los dominios que utiliza en “Return-Path” (Ruta de devolución) o en la dirección “Reply-to” (Responder a).
- Amazon SES está disponible en distintas regiones de AWS. Si utiliza más de una región de AWS para enviar un correo electrónico, tiene que completar el proceso de configuración de DKIM en cada una de esas regiones para garantizar que todos sus correos electrónicos se firmen con DKIM.
- Ya que las propiedades DKIM se heredan del dominio principal, cuando se verifica un dominio con autenticación DKIM:
  - La autenticación DKIM también se aplicará a todos los subdominios de ese dominio.

    - La configuración de DKIM para un subdominio puede anular la configuración del dominio principal al desactivar la herencia si no desea que el subdominio utilice la autenticación DKIM, así como la posibilidad de volver a habilitarla posteriormente.
- La autenticación DKIM también se aplicará a todo el correo electrónico enviado desde una identidad de correo electrónico que haga referencia al dominio verificado por DKIM en su dirección.
    - La configuración de DKIM para una dirección de correo electrónico puede anular la configuración del subdominio (si procede) y del dominio principal, al desactivar la herencia si desea enviar correo sin autenticación DKIM, así como la posibilidad de volver a habilitarla más adelante.

Descripción de las propiedades de firma DKIM heredadas

Es importante entender en primer lugar que una identidad de dirección de correo electrónico hereda sus propiedades de firma DKIM de su dominio principal si ese dominio se configuró con DKIM, independientemente de si se utilizó Easy DKIM o BYODKIM. Por lo tanto, la desactivación o habilitación de la firma DKIM en la identidad de la dirección de correo electrónico anula las propiedades de firma DKIM del dominio, con base en los siguientes hechos clave:

- Si ya ha configurado DKIM para el dominio al que pertenece la dirección de correo electrónico, no es necesario que también configure la firma DKIM para la dirección de correo electrónico.
    - A la hora de configurar DKIM para un dominio, Amazon SES autentica automáticamente cada correo electrónico de cada dirección en ese dominio mediante las propiedades DKIM heredadas del dominio principal.
- La configuración de DKIM para una identidad de dirección de correo electrónico específica anula automáticamente las configuraciones del dominio principal o subdominio (si corresponde) al que pertenece la dirección.

Dado que las propiedades de firma DKIM de la identidad de la dirección de correo electrónico se heredan del dominio principal, si planea anular estas propiedades, debe tener en cuenta las reglas jerárquicas de anulación, tal como se explica en la tabla siguiente.

El dominio principal no tiene habilitada la firma DKIM	El dominio principal tiene habilitada la firma DKIM
No se puede habilitar la firma DKIM en la identidad de la dirección de correo electrónico.	Puede desactivar la firma DKIM en la identidad de la dirección de correo electrónico.
	Puede volver a habilitar la firma DKIM en la identidad de la dirección de correo electrónico.

Por lo general, nunca se recomienda desactivar la firma DKIM, ya que podría perjudicar la reputación del remitente y aumenta el riesgo de que el correo enviado vaya a carpetas de correo no deseado o spam o que suplanten el dominio.

Sin embargo, existe la capacidad de anular las propiedades de firma DKIM heredadas del dominio en una identidad de dirección de correo electrónico para cualquier caso de uso concreto o decisión empresarial subyacente en las que tenga que desactivar de forma permanente o temporal la firma DKIM, o volver a habilitarla más adelante. Consulte the section called “Anulación de la firma DKIM en una de dirección de correo electrónico”.

Easy DKIM en Amazon SES

A la hora de configurar Easy DKIM para una identidad de dominio, Amazon SES agrega automáticamente una clave DKIM de 2048 bits a cada correo electrónico que envíe desde dicha identidad. Puede configurar Easy DKIM mediante la consola de Amazon SES o mediante la API.

> **Note**
>
> Para configurar Easy DKIM, es necesario modificar la configuración de DNS del dominio. Si utiliza Route 53 como su proveedor de DNS, Amazon SES puede crear automáticamente los registros adecuados para usted. Si utiliza otro proveedor de DNS, consulte la documentación del proveedor para obtener más información sobre cómo cambiar la configuración de DNS de su dominio.

> **Warning**
>
> Si actualmente tiene BYODKIM habilitado y está haciendo la transición a Easy DKIM, tenga en cuenta que Amazon SES no utilizará BYODKIM para firmar los correos electrónicos

mientras se está configurando Easy DKIM y el estado de DKIM esté pendiente. Desde el momento en que realiza la llamada para habilitar Easy DKIM (ya sea a través de la API o la consola) y el momento en que SES puede confirmar la configuración de DNS, SES puede enviar los correos electrónicos sin firma de DKIM. Por lo tanto, se recomienda utilizar un paso intermedio para migrar de un método de firma de DKIM a otro (por ejemplo, utilizar un subdominio del dominio con BYODKIM habilitado y luego eliminarlo una vez que se haya superado la verificación de Easy DKIM) o realizar esta actividad durante el tiempo de inactividad de la aplicación, si lo hubiera.

Cómo configurar Easy DKIM para una identidad de dominio verificada

El procedimiento de esta sección es más simple y sólo muestra los pasos necesarios para configurar Easy DKIM en una identidad de dominio que ya creó. Si aun no ha creado una identidad de dominio o quiere ver todas las opciones disponibles de personalización de una identidad de dominio, como el uso de un conjunto de configuración predeterminado, un dominio MAIL FROM personalizado y etiquetas, consulte the section called “Creación de una identidad de dominio”.

Parte de la creación de una identidad de dominio Easy DKIM consiste en configurar su verificación basada en DKIM, en la que tendrá la opción de aceptar el valor predeterminado de Amazon SES de 2048 bits o de sobrescribir el valor predeterminado seleccionando la opción de 1024 bits. Consulte the section called “Longitud de clave de firma de DKIM” para obtener más información acerca de las longitudes de clave de firma DKIM y cómo cambiarlas.

Para configurara Easy DKIM para un dominio

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).
3. En la lista de identidades, elija una identidad en la que el Identity type (Tipo de identidad)sea Domain (Dominio).

> **Note**
>
> Si necesita crear o verificar un dominio, consulte Creación de una identidad de dominio.

4. En la pestaña Authentication (Autenticación), en el contenedor DomainKeys Identified Mail (DKIM) (Correo identificado con claves de dominio) (DKIM), elija Edit (Editar).
5. En el contenedor Configuración avanzada de DKIM, elija el botón Easy DKIM en el campo Tipo de identidad.
6. En el campo DKIM signing key length (Longitud de clave de firma de DKIM), elija RSA_2048_BIT o RSA_1024_BIT.
7. En el campo DKIM signatures (Firmas DKIM), active la casilla Enabled (Habilitada).
8. Elija Save changes.
9. Ahora que ha configurado la identidad de dominio con Easy DKIM, debe completar el proceso de verificación con el proveedor de DNS; continuar con the section called “Verificación de una identidad de dominio” y seguir los procedimientos de autenticación de DNS para Easy DKIM.

Cambiar la longitud de la clave de firma Easy DKIM para una identidad

El procedimiento que se describe en esta sección muestra cómo puede cambiar fácilmente los bits de Easy DKIM necesarios para el algoritmo de firma. Aunque siempre es preferible utilizar una longitud de firma de 2048 bits por la mayor seguridad que proporciona, puede haber situaciones que requieran utilizar la longitud de 1024 bits, como, por ejemplo, cuando tenga que utilizar un proveedor de DNS que solo admita DKIM 1024.

Para preservar la capacidad de entrega del correo electrónico en tránsito, existen restricciones sobre la frecuencia con la que puede cambiar o intercambiar la longitud de la clave DKIM.

Cuando el correo electrónico está en tránsito, el DNS utiliza su clave pública para autenticar el correo electrónico; por lo tanto, si cambia las claves con demasiada rapidez o frecuencia, es posible que el DNS no pueda autenticar con DKIM el correo electrónico, ya que es posible que la clave anterior ya esté invalidada. Las restricciones que se describen a continuación evitan este problema:

- No se puede cambiar a la misma longitud de clave que la que ya está configurada.
- No se puede cambiar a una longitud de clave diferente más de una vez en un período de 24 horas (a menos que sea la primera actualización a 1024 en dicho período).

Al utilizar los siguientes procedimientos para cambiar la longitud de la clave, si infringe una de estas restricciones, la consola mostrará un banner de error para indicar que la entrada que proporcionó no es válida junto con la razón de por qué no era válida.

Para cambiar los bits de longitud de clave de firma DKIM

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).
3. En la lista de identidades, elija la identidad para la que desea cambiar la longitud de clave de firma DKIM.
4. En la pestaña Authentication (Autenticación), en el contenedor DomainKeys Identified Mail (DKIM) (Correo identificado con claves de dominio) (DKIM), elija Edit (Editar).
5. En el contenedor Advanced DKIM settings (Configuración avanzada de DKIM), elija entre RSA_2048_BIT o RSA_1024_BIT en el campo DKIM signing key length (Longitud de clave de firma DKIM).
6. Elija Save changes.

Uso de su propio token de autenticación (BYODKIM) de DKIM en Amazon SES

En lugar de usar Easy DKIM, puede configurar la autenticación de DKIM con su propio par de claves públicas-privadas. Este proceso se conoce como Utilice su propio DKIM (BYODKIM).

Con BYODKIM, puede utilizar un solo registro DNS para configurar la autenticación de DKIM de sus dominios, a diferencia de Easy DKIM, que requiere que publique tres registros DNS independientes. Además, con BYODKIM, podrá rotar las claves DKIM de sus dominios tantas veces como desee.

Temas de esta sección:

- Paso 1: Crear el par de claves
- Paso 2: Agregar la clave pública y el selector a la configuración de DNS del dominio
- Paso 3: Configurar y verificar un dominio para usar BYODKIM

> **Warning**
>
> Si actualmente tiene Easy DKIM habilitado y está haciendo la transición a BYODKIM, tenga en cuenta que Amazon SES no utilizará Easy DKIM para firmar los correos electrónicos mientras se está configurando BYODKIM y el estado de DKIM está pendiente. Desde el momento en que realiza la llamada para habilitar BYODKIM (ya sea a través de la API o la

consola) y el momento en que SES puede confirmar la configuración de DNS, SES puede enviar los correos electrónicos sin firma de DKIM. Por lo tanto, se recomienda utilizar un paso intermedio para migrar de un método de firma de DKIM a otro (por ejemplo, utilizar un subdominio del dominio con Easy DKIM habilitado y luego eliminarlo una vez que se haya superado la verificación de BYODKIM) o realizar esta actividad durante el tiempo de inactividad de la aplicación, si lo hubiera.

Paso 1: Crear el par de claves

Para utilizar la característica de uso de DKIM propio, primero debe crear un par de claves RSA.

La clave privada que genere tiene que estar en formato PKCS #1 o PKCS #8, debe utilizar al menos un cifrado RSA de 1024 bits y hasta 2048 bits y debe estar codificada con base64 (PEM). Consulte the section called “Longitud de clave de firma de DKIM” para obtener más información acerca de las longitudes de clave de firma DKIM y cómo cambiarlas.

> **Note**
>
> Puede usar aplicaciones y herramientas de terceros para generar pares de claves RSA siempre que la clave privada se genere con al menos un cifrado RSA de 1024 bits y de hasta 2048 bits, y esté codificada con base64 (PEM).

En el siguiente procedimiento, el código de ejemplo que utiliza el comando `openssl genrsa` integrado en la mayoría de los sistemas operativos Linux, macOS o Unix para crear el par de claves utilizará automáticamente codificación base64 (PEM).

Para crear el par de claves desde la línea de comandos de Linux, macOS o Unix

1. En la línea de comandos, ingrese el comando siguiente para generar la clave privada reemplazando *nnnn* con una longitud de bits de al menos 1024 bits y hasta 2048 bits:

   ```
   openssl genrsa -f4 -out private.key nnnn
   ```

2. En la línea de comandos, escriba el comando siguiente para generar la clave pública:

   ```
   openssl rsa -in private.key -outform PEM -pubout -out public.key
   ```

Paso 2: Agregar la clave pública y el selector a la configuración de DNS del dominio

Ahora que ha creado un par de claves, debe agregar la clave pública como registro TXT a la configuración de DNS de su dominio.

Para añadir la clave pública a la configuración de DNS de su dominio

1. Inicie sesión en la consola de administración del proveedor de DNS o de alojamiento.
2. Añada un nuevo registro de texto a la configuración de DNS de su dominio. El registro debe usar el siguiente formato:

Nombre	Tipo	Valor
selector._domainkey.*example.com*	TXT	p=*yourPublicKey*

En el ejemplo anterior, realice los siguientes cambios:

- Reemplace *selector* por un nombre único que identifique la clave.

> **Note**
>
> Un pequeño número de proveedores de DNS no le permiten incluir guiones bajos (_) en los nombres de registro. Sin embargo, el guion bajo el nombre de registro de DKIM es obligatorio. Si su proveedor de DNS no le permite introducir un guion bajo en el nombre del registro, póngase en contacto con el equipo de atención al cliente del proveedor para obtener ayuda.

- Reemplace *example.com* por su dominio.
- Reemplace *yourPublicKey* con la clave pública que creó anteriormente e incluya el prefijo p= tal y como se muestra en la columna Value (Valor) anterior.

> **Note**
>
> Cuando publica (agrega) su clave pública a su proveedor de DNS, debe tener el siguiente formato:

- Debe eliminar la primera y la última línea (`-----BEGIN PUBLIC KEY-----` y `-----END PUBLIC KEY-----`, respectivamente) de la clave pública generada. Además, debe eliminar los saltos de línea en la clave pública generada. El valor resultante es una cadena de caracteres sin espacios ni saltos de línea.
- Debe incluir en prefijo p= tal y como se muestra en la columna Value (Valor) de la tabla anterior.

Cada proveedor tiene diferentes procedimientos para actualizar los registros de DNS. La tabla que sigue incluye enlaces a la documentación de unos pocos proveedores de DNS muy utilizados. Esta lista no es exhaustiva y no implica aprobación; del mismo modo, si su proveedor de DNS no aparece en la lista, no implica que no pueda usar el dominio con Amazon SES.

Proveedor de DNS/alojamiento	Enlace a la documentación
Amazon Route 53	Edición de registros en la Guía para desarrolladores de Amazon Route 53
GoDaddy	Añadir un registro TXT (enlace externo)
DreamHost	How do I add custom DNS records? (enlace externo)
Cloudflare	Managing DNS records in CloudFlare (enlace externo)
HostGator	Manage DNS Records with HostGator/eNom (enlace externo)
Namecheap	How do I add TXT/SPF/DKIM/DMARC records for my domain? (enlace externo)
Names.co.uk	Changing your domains DNS Settings (enlace externo)
Wix	Adding or Updating TXT Records in Your Wix Account (enlace externo)

Paso 3: Configurar y verificar un dominio para usar BYODKIM

Puede configurar BYODKIM tanto para los dominios nuevos (es decir, los dominios que no utiliza actualmente para enviar correo electrónico a través Amazon SES) como para los dominios existentes (es decir, los dominios que ya ha configurado para utilizar con Amazon SES) mediante la consola o la AWS CLI. Antes de utilizar los procedimientos de la AWS CLI que se describen en esta sección, primero debe instalar y configurar la AWS CLI. Para obtener más información, consulte la Guía del usuario de AWS Command Line Interface.

Opción 1: Crear una nueva identidad de dominio que utiliza BYODKIM

Esta sección contiene procedimientos para crear una nueva identidad de dominio que utiliza BYODKIM. Una nueva identidad de dominio es un dominio que no ha configurado previamente para enviar correo electrónico mediante Amazon SES.

Si desea configurar un dominio existente para utilizar BYODKIM, complete el procedimiento de Opción 2: Configuración de una identidad de dominio existente en su lugar.

Para crear una identidad mediante BYODKIM desde la consola

- Siga los procedimientos indicados en Creación de una identidad de dominio, y cuando llegue al paso 8, siga las instrucciones específicas para BYODKIM.

Para crear una identidad mediante BYODKIM desde la AWS CLI

Para configurar un nuevo dominio, utilice la operación `CreateEmailIdentity` de la API de Amazon SES.

1. En el editor de texto, pegue el siguiente código:

```
{
    "EmailIdentity":"example.com",
    "DkimSigningAttributes":{
        "DomainSigningPrivateKey":"privateKey",
        "DomainSigningSelector":"selector"
    }
}
```

   En el ejemplo anterior, realice los siguientes cambios:

   - Reemplace *example.com* por el dominio que desea crear.

- Reemplace *privateKey* por su clave privada.

> **Note**
>
> Debe eliminar la primera y la última línea (`-----BEGIN PRIVATE KEY-----` y `-----END PRIVATE KEY-----`, respectivamente) de la clave privada generada. Además, debe eliminar los saltos de línea en la clave privada generada. El valor resultante es una cadena de caracteres sin espacios ni saltos de línea.

- Reemplace *selector* por el selector único que especificó al crear el registro TXT en la configuración de DNS de su dominio.

Cuando haya terminado, guarde el archivo como `create-identity.json`.

2. En la línea de comandos, escriba el comando siguiente.

```
aws sesv2 create-email-identity --cli-input-json file://path/to/create-identity.json
```

En el comando anterior, reemplace *path/to/create-identity.json* por la ruta completa al archivo que creó en el paso anterior.

Opción 2: Configuración de una identidad de dominio existente

Esta sección contiene procedimientos para actualizar una identidad de dominio existente para utilizar BYODKIM. Una identidad de dominio existente es un dominio que ya ha configurado para enviar correo electrónico mediante Amazon SES.

Para actualizar una identidad de dominio mediante BYODKIM desde la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).
3. En la lista de identidades, elija una identidad en la que el Identity type (Tipo de identidad)sea Domain (Dominio).

> **Note**
>
> Si necesita crear o verificar un dominio, consulte Creación de una identidad de dominio.

4. En la pestaña Authentication (Autenticación), en el panel DomainKeys Identified Mail (DKIM), (Correo identificado con claves de dominio) (DKIM), elija Edit (Editar).
5. En el panel Advanced DKIM settings (Configuración avanzada de DKIM), elija el botón Provide DKIM authentication token (BYODKIM) [Proporcionar token de autenticación DKIM (BYODKIM)] en el campo Identity type (Tipo de identidad).
6. Pegue en Private key (Clave privada) la clave privada que generó anteriormente.

> **Note**
>
> Debe eliminar la primera y la última línea (`-----BEGIN PRIVATE KEY-----` y `-----END PRIVATE KEY-----`, respectivamente) de la clave privada generada. Además, debe eliminar los saltos de línea en la clave privada generada. El valor resultante es una cadena de caracteres sin espacios ni saltos de línea.

7. En Selector name (Nombre del selector), ingrese el nombre del selector que especificó en la configuración de DNS de su dominio.
8. En el campo DKIM signatures (Firmas DKIM), active la casilla Enabled (Habilitada).
9. Elija Save changes (Guardar cambios).

Para actualizar una identidad de dominio mediante BYODKIM desde la AWS CLI

Para configurar un dominio existente, utilice la operación `PutEmailIdentityDkimSigningAttributes` de la API de Amazon SES.

1. En el editor de texto, pegue el siguiente código:

```
{
    "SigningAttributes":{
        "DomainSigningPrivateKey":"privateKey",
        "DomainSigningSelector":"selector"
    },
    "SigningAttributesOrigin":"EXTERNAL"
}
```

En el ejemplo anterior, realice los siguientes cambios:

- Reemplace *privateKey* por su clave privada.

> **Note**
>
> Debe eliminar la primera y la última línea (`-----BEGIN PRIVATE KEY-----` y `-----END PRIVATE KEY-----`, respectivamente) de la clave privada generada. Además, debe eliminar los saltos de línea en la clave privada generada. El valor resultante es una cadena de caracteres sin espacios ni saltos de línea.

- Reemplace *selector* por el selector único que especificó al crear el registro TXT en la configuración de DNS de su dominio.

Cuando haya terminado, guarde el archivo como `update-identity.json`.

2. En la línea de comandos, escriba el comando siguiente.

```
aws sesv2 put-email-identity-dkim-signing-attributes --email-identity example.com
 --cli-input-json file://path/to/update-identity.json
```

En el comando anterior, realice los siguientes cambios:

- Reemplace *path/to/update-identity.json* por la ruta completa al archivo que creó en el paso anterior.
- Reemplace *example.com* por el dominio que desea actualizar.

Verificación del estado de DKIM de un dominio que utiliza BYODKIM

Para verificar el estado de DKIM de un dominio desde la consola

Después de configurar un dominio para utilizar BYODKIM, puede utilizar la consola SES para verificar que DKIM se haya configurado correctamente.

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).

3. En la lista de identidades, elija la identidad cuyo estado de DKIM desee verificar.
4. Los cambios en la configuración del DNS pueden tardar hasta 72 horas en propagarse. Tan pronto como Amazon SES detecte todos los registros DKIM requeridos en la configuración DNS de su dominio, el proceso de verificación quedará completado. Si todo se ha configurado correctamente, el campo DKIM configuration (Configuración de DKIM) del dominio mostrará Successful (Correcto) en el panel DomainKeys Identified Mail (DKIM) [Correo identificado de claves de dominio (DKIM)], y el campo Identity status (Estado de identidad) mostrará Verified (Verificado) en el panel Summary (Resumen).

Para verificar el estado de DKIM de un dominio mediante la AWS CLI

Después de configurar un dominio para utilizar BYODKIM, puede utilizar la operación GetEmailIdentity para verificar que DKIM se haya configurado correctamente.

- En la línea de comandos, escriba el comando siguiente.

  ```
  aws sesv2 get-email-identity --email-identity example.com
  ```

  En el comando anterior, reemplace *example.com* por su dominio.

  Este comando devuelve un objeto JSON que contiene una sección similar al siguiente ejemplo.

  ```
  {
      ...
      "DkimAttributes": {
          "SigningAttributesOrigin": "EXTERNAL",
          "SigningEnabled": true,
          "Status": "SUCCESS",
          "Tokens": [ ]
      },
      ...
  }
  ```

  Si todo lo que se describe a continuación es verdadero, BYODKIM se ha configurado correctamente para el dominio:

  - El valor de la propiedad `SigningAttributesOrigin` es `EXTERNAL`.
  - El valor de `SigningEnabled` es `true`.
  - El valor de `Status` es `SUCCESS`.

Gestión de Easy DKIM y BYODKIM

Puede administrar la configuración de DKIM para sus identidades autenticadas con Easy DKIM o BYODKIM mediante la consola de Amazon SES basada en la web o mediante la API de Amazon SES. Puede utilizar cualquiera de estos métodos para obtener los registros de DKIM para una identidad, o para habilitar o desactivar la firma DKIM de una identidad.

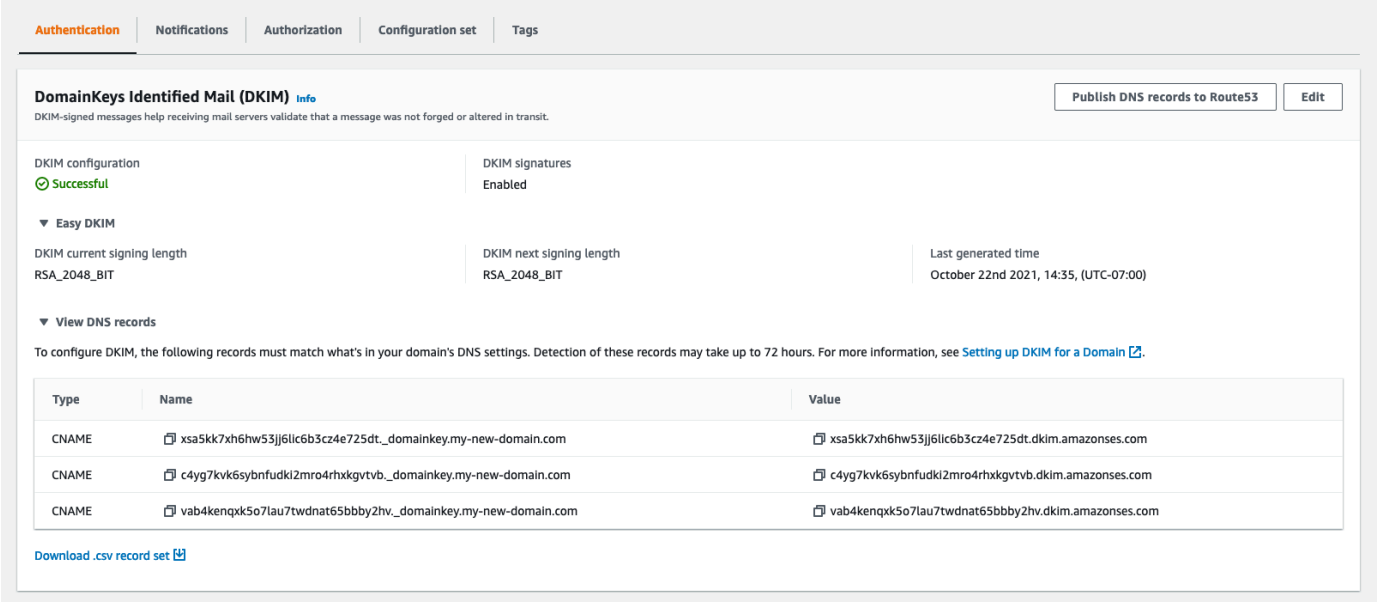
Obtención de registros de DKIM para una identidad

Puede obtener los registros de DKIM para su dominio o la dirección de correo electrónico en cualquier momento mediante la consola de Amazon SES.

Para obtener los registros de DKIM para una identidad mediante la consola

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).
3. En la lista de identidades, elija la identidad para la que desea obtener los registros de DKIM.
4. En la pestaña Authentication (Autenticación) de la página de detalles de identidad, expanda View DNS records (Ver registros DNS).
5. Copie los tres registros CNAME si utilizó Easy DKIM, o el registro TXT si utilizó BYODKIM, que aparecen en esta sección. También puede elegir Download .csv record set (Descargar el conjunto de registro .csv) para guardar una copia de los registros en su computadora.

   La siguiente imagen muestra un ejemplo de la sección ampliada View DNS records (Ver registros DNS) que muestra los registros CNAME asociados a Easy DKIM.



También puede obtener los registros de DKIM para una identidad mediante la API de Amazon SES. Un método común de interactuar con la API es utilizar el AWS CLI.

Para obtener los registros DKIM de una identidad mediante el AWS CLI

1. En la línea de comando, escriba el comando siguiente:

   ```
   aws ses get-identity-dkim-attributes --identities "example.com"
   ```

   En el siguiente ejemplo, sustituya *example.com* por la identidad de la que desea obtener registros de DKIM. Puede especificar una dirección de correo electrónico o un dominio.

2. El resultado de este comando contiene una sección de `DkimTokens`, tal y como se muestra en el siguiente ejemplo:

   ```
   {
       "DkimAttributes": {
           "example.com": {
               "DkimEnabled": true,
               "DkimVerificationStatus": "Success",
               "DkimTokens": [
                   "hirjd4exampled5477y22yd23ettobi",
                   "v3rnz522czcl46quexamplek3efo5o6x",
                   "y4examplexbhyhnsjcmtvzotfvqjmdqoj"
               ]
   ```

```
        }
    }
}
```

Puede utilizar los tokens para crear los registros de CNAME que añade a la configuración de DNS de su dominio. Para crear los registros de CNAME, utilice la siguiente plantilla:

```
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
```

Reemplace cada instancia de *token1* con el primer token en la lista que recibió cuando ejecutó el comando `get-identity-dkim-attributes`, reemplace todas las instancias de *token2* con el segundo token en la lista y reemplace todas las instancias de *token3* con el tercer token en la lista.

Por ejemplo, la aplicación de esta plantilla a los tokens que se muestran en el anterior ejemplo produce los siguientes registros:

```
hirjd4exampled5477y22yd23ettobi._domainkey.example.com CNAME
 hirjd4exampled5477y22yd23ettobi.dkim.amazonses.com
v3rnz522czcl46quexamplek3efo5o6x._domainkey.example.com CNAME
 v3rnz522czcl46quexamplek3efo5o6x.dkim.amazonses.com
y4examplexbhyhnsjcmtvzotfvqjmdqoj._domainkey.example.com CNAME
 y4examplexbhyhnsjcmtvzotfvqjmdqoj.dkim.amazonses.com
```

> **Note**
>
> Si ha seleccionado Región de AWS Ciudad del Cabo, Osaka o Milán, necesitará usar dominios DKIM específicos de la región, tal y como se especifica en la tabla de dominios DKIM que se encuentra en el. Referencia general de AWS

Desactivación de Easy DKIM para una identidad

Puede desactivar rápidamente la autenticación DKIM para una identidad mediante la consola de Amazon SES.

Para desactivar DKIM para una identidad

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).
3. En la lista de identidades, elija la identidad para la que desea desactivar los registros de DKIM.
4. En la pestaña Autenticación, en el contenedor de correo DomainKeys identificado (DKIM), selecciona Editar.
5. En Advanced DKIM settings (Configuración avanzada de DKIM), desmarque la casilla Enabled (Habilitado) en el cuadro de diálogo DKIM signatures (Firmas DKIM).

También puede desactivar DKIM para una identidad mediante la API de Amazon SES. Un método común de interactuar con la API es utilizar el AWS CLI.

Para deshabilitar el DKIM para una identidad mediante el AWS CLI

- En la línea de comando, escriba el comando siguiente:

  ```
  aws ses set-identity-dkim-enabled --identity example.com --no-dkim-enabled
  ```

  En el siguiente ejemplo, sustituya *example.com* por la identidad para la que desea desactivar los registros de DKIM. Puede especificar una dirección de correo electrónico o un dominio.

Habilitación de Easy DKIM para una identidad

Si previamente ha desactivado DKIM para una identidad, puede habilitarlo de nuevo mediante la consola de Amazon SES.

Para habilitar DKIM para una identidad

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).
3. En la lista de identidades, elija la identidad para la que desea habilitar los registros de DKIM.

4. En la pestaña Autenticación, en el contenedor de correo DomainKeys identificado (DKIM), selecciona Editar.
5. En Advanced DKIM settings (Configuración avanzada de DKIM), active la casilla Enabled (Habilitado) en el cuadro de diálogo DKIM signatures (Firmas DKIM).

También puede habilitar DKIM para una identidad mediante la API de Amazon SES. Un método común de interactuar con la API es utilizar el AWS CLI.

Para habilitar el DKIM para una identidad mediante el AWS CLI

- En la línea de comando, escriba el comando siguiente:

```
aws ses set-identity-dkim-enabled --identity example.com --dkim-enabled
```

  En el siguiente ejemplo, sustituya *example.com* por la identidad para la que desea habilitar los registros de DKIM. Puede especificar una dirección de correo electrónico o un dominio.

Anulación de la firma DKIM heredada en una identidad de dirección de correo electrónico

En esta sección aprenderá a anular (desactivar o habilitar) las propiedades de firma de DKIM heredadas del dominio principal en una identidad de dirección de correo electrónico específica que ya haya verificado con Amazon SES. Solo puede hacerlo para las identidades de dirección de correo electrónico que pertenecen a dominios que ya posea porque la configuración de DNS se configura a nivel de dominio.

Important

No puede desactivar o habilitar la firma DKIM para las identidades de direcciones de correo electrónico:

- en dominios que no le pertenecen Por ejemplo, no puede alternar la firma DKIM para una dirección gmail.com o hotmail.com,
- en dominios que le pertenecen, pero que aún no se han verificado en Amazon SES
- en dominios que le pertenecen, pero para los que no se ha habilitado la firma DKIM en el dominio.

Esta sección contiene los siguientes temas:

- Descripción de las propiedades de firma DKIM heredadas
- Anulación de la firma DKIM heredada en una identidad de dirección de correo electrónico (consola)
- Anulación de la firma DKIM heredada en una identidad de dirección de correo electrónico (AWS CLI)

Descripción de las propiedades de firma DKIM heredadas

Es importante entender en primer lugar que una identidad de dirección de correo electrónico hereda sus propiedades de firma DKIM de su dominio principal si ese dominio se configuró con DKIM, independientemente de si se utilizó Easy DKIM o BYODKIM. Por lo tanto, la desactivación o habilitación de la firma DKIM en la identidad de la dirección de correo electrónico anula las propiedades de firma DKIM del dominio, con base en los siguientes hechos clave:

- Si ya ha configurado DKIM para el dominio al que pertenece la dirección de correo electrónico, no es necesario que también configure la firma DKIM para la dirección de correo electrónico.
  - A la hora de configurar DKIM para un dominio, Amazon SES autentica automáticamente cada correo electrónico de cada dirección en ese dominio mediante las propiedades DKIM heredadas del dominio principal.
- La configuración de DKIM para una identidad de dirección de correo electrónico específica anula automáticamente las configuraciones del dominio principal o subdominio (si corresponde) al que pertenece la dirección.

Dado que las propiedades de firma DKIM de la identidad de la dirección de correo electrónico se heredan del dominio principal, si planea anular estas propiedades, debe tener en cuenta las reglas jerárquicas de anulación, tal como se explica en la tabla siguiente.

El dominio principal no tiene habilitada la firma DKIM	El dominio principal tiene habilitada la firma DKIM
No se puede habilitar la firma DKIM en la identidad de la dirección de correo electrónico.	Puede desactivar la firma DKIM en la identidad de la dirección de correo electrónico.
	Puede volver a habilitar la firma DKIM en la identidad de la dirección de correo electrónico.

Por lo general, nunca se recomienda desactivar la firma DKIM, ya que podría perjudicar la reputación del remitente y aumenta el riesgo de que el correo enviado vaya a carpetas de correo no deseado o spam o que suplanten el dominio.

Sin embargo, existe la capacidad de anular las propiedades de firma DKIM heredadas del dominio en una identidad de dirección de correo electrónico para cualquier caso de uso concreto o decisión empresarial subyacente en las que tenga que desactivar de forma permanente o temporal la firma DKIM, o volver a habilitarla más adelante.

Anulación de la firma DKIM heredada en una identidad de dirección de correo electrónico (consola)

En el siguiente procedimiento de la consola de SES, se explica cómo anular (desactivar o habilitar) las propiedades de firma DKIM heredadas del dominio principal en una identidad de dirección de correo electrónico específica que ya verificó con Amazon SES.

Para desactivar o habilitar la firma DKIM para una identidad de dirección de correo electrónico mediante la consola

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).
3. En la lista de identidades, elija una identidad donde Identity type (Tipo de identidad) sea Email address (Dirección de correo electrónico) y pertenezca a uno de sus dominios verificados.
4. En la pestaña Autenticación, en el contenedor de correo DomainKeys identificado (DKIM), selecciona Editar.

   > **Note**
   >
   > La pestaña Authentication (Autenticación) solo está presente si la identidad de la dirección de correo electrónico seleccionada pertenece a un dominio que SES ya ha verificado. Si todavía no ha verificado su dominio, consulte Creación de una identidad de dominio.

5. En Advanced DKIM settings (Configuración avanzada de DKIM), en el campo DKIM signatures (Firmas de DKIM), desmarque la casilla Enabled (Habilitado) para desactivar la firma DKIM o selecciónela a fin de volver a habilitar la firma DKIM (si se había anulado anteriormente).
6. Elija Guardar cambios.

Anulación de la firma DKIM heredada en una identidad de dirección de correo electrónico (AWS CLI)

En el siguiente ejemplo, se utiliza un comando y parámetros de la AWS CLI API de SES que anularán (deshabilitarán o habilitarán) las propiedades de firma DKIM heredadas del dominio principal en una identidad de dirección de correo electrónico específica que ya haya verificado con SES.

Para desactivar o habilitar la firma DKIM para una identidad de dirección de correo electrónico mediante la AWS CLI

- Suponiendo que usted sea el titular del dominio example.com y desea desactivar la firma DKIM para una de las direcciones de correo electrónico del dominio, en la línea de comandos, escriba el siguiente comando:

```
aws sesv2 put-email-identity-dkim-attributes --email-identity marketing@example.com
 --no-signing-enabled
```

  a. Reemplace *marketing@example.com* con la identidad de dirección de correo electrónico para la que desea desactivar la firma DKIM.

  b. `--no-signing-enabled` desactivará la firma DKIM. Para volver a habilitar la firma DKIM, utilice `--signing-enabled`.

Firma DKIM manual en Amazon SES

Como alternativa al uso de Easy DKIM, puede agregar manualmente firmas DKIM para sus mensajes y enviar esos mensajes a través de Amazon SES. Si decide firmar sus mensajes de forma manual, primero debe crear una firma DKIM. Después de crear el mensaje y la firma DKIM, puede utilizar la API SendRawEmail para enviarlo.

Si decide firmar su correo electrónico de forma manual, tenga en cuenta los siguientes factores:

- Cada mensaje que envíe mediante Amazon SES contiene un encabezado DKIM que hace referencia a un dominio de firma de amazonses.com (es decir, contiene la siguiente cadena: `d=amazonses.com`). Por lo tanto, si firma sus mensajes de forma manual, sus mensajes incluirán dos encabezados DKIM: uno para su dominio y el que cree automáticamente Amazon SES para amazonses.com.

- Amazon SES no valida las firmas DKIM que agregue de forma manual a sus mensajes. Si hay errores con la firma DKIM en un mensaje, puede ser rechazado por los proveedores de correo electrónico..
- Cuando firma sus mensajes, debe utilizar una longitud bits de al menos 1024 bits.
- No firme los siguientes campos: ID de mensaje, fecha, ruta de retorno (Return-Path), reenvío de devolución (Bounces-To).

> **Note**
>
> Si utiliza un cliente de correo electrónico para enviar correo electrónico a través de la interfaz SMTP de Amazon SES, el cliente puede realizar automáticamente la firma DKIM de sus mensajes. Algunos clientes podrían firmar algunos de estos campos. Para obtener información acerca de los campos que se firman de forma predeterminada, consulte la documentación de su cliente de correo electrónico.

Autenticación de correo electrónico con SPF en Amazon SES

El marco de directivas de remitente (SPF) es un estándar de validación de correo electrónico que ha sido diseñado para prevenir la suplantación de correo electrónico. Los propietarios de dominios utilizan SPF para indicar a los proveedores de correo electrónico qué servidores pueden enviar correo electrónico desde sus dominios. SPF se define en RFC 7208.

Los mensajes que envíe a través de Amazon SES automáticamente utilizan un subdominio de `amazonses.com` como el dominio MAIL FROM predeterminado. La autenticación de SPF valida correctamente estos mensajes porque el dominio MAIL FROM predeterminado coincide con la aplicación que envió el correo electrónico, en este caso, SES. Por lo tanto, en SES, el SPF está configurado implícitamente para usted.

Sin embargo, si no quieres usar el dominio MAIL FROM predeterminado de SES y prefieres usar un subdominio de un dominio de tu propiedad, en SES se denomina usar un dominio MAIL FROM personalizado. Para ello, es necesario que publique su propio registro SPF para el dominio MAIL FROM personalizado. Además, SES también le exige que configure un registro de MX para que el dominio MAIL FROM personalizado pueda recibir las notificaciones de rebotes y reclamaciones que los proveedores de correo electrónico le envían.

Aprenda a configurar la autenticación SPF

Se proporcionan instrucciones para configurar tu dominio con SPF y cómo publicar en él los registros MX y SPF (tipo TXT). the section called “Uso de un dominio MAIL FROM personalizado”

Uso de un dominio MAIL FROM personalizado

Cuando se envía un correo electrónico, tiene dos direcciones que indican su origen: una dirección From que se muestra al destinatario del mensaje y una dirección MAIL FROM que indica dónde se originó el mensaje. La dirección MAIL FROM a veces recibe el nombre de dirección envelope sender, envelope from, bounce address o Return Path. Los servidores de correo utilizan la dirección MAIL FROM para devolver mensajes de rebote y otras notificaciones de error. Normalmente, los destinatarios solo pueden ver la dirección MAIL FROM si ven el código fuente del mensaje.

Amazon SES establece el dominio MAIL FROM para los mensajes que envía a un valor predeterminado a menos que especifique su propio dominio (personalizado). En esta sección se explican los beneficios de configurar un dominio MAIL FROM personalizado y se incluyen procedimientos de configuración.

Razones para utilizar un dominio MAIL FROM personalizado

Los mensajes que envíe a través de Amazon SES automáticamente utilizan un subdominio de `amazonses.com` como el dominio MAIL FROM predeterminado. La autenticación del marco de políticas de remitentes (SPF) valida correctamente estos mensajes porque el dominio MAIL FROM predeterminado coincide con la aplicación que envió el correo electrónico, en este caso, SES.

Si no quiere usar el dominio MAIL FROM predeterminado de SES y prefiere usar un subdominio de un dominio de su propiedad, en SES se denomina uso de un dominio MAIL FROM personalizado. Para ello, es necesario que publique su propio registro SPF para el dominio MAIL FROM personalizado. Además, SES también le exige que configure un registro de MX para que el dominio pueda recibir las notificaciones de rebotes y reclamaciones que los proveedores de correo electrónico le envían.

Al usar un dominio MAIL FROM personalizado, tiene la flexibilidad de usar SPF, DKIM o ambos para lograr la validación Autenticación, informe y conformidad del mensaje basado en el dominio (DMARC). DMARC permite al dominio de un remitente indicar que los correos electrónicos enviados desde el dominio están protegidos por uno o varios sistemas de autenticación. Existen dos maneras de conseguir la validación de DMARC: the section called “Conformidad con DMARC a través de SPF” y the section called “Conformidad con DMARC a través de DKIM”.

Elección de un dominio MAIL FROM personalizado

A continuación, el término dominio MAIL FROM siempre se refiere a un subdominio de un dominio que sea de tu propiedad; este subdominio que utilices para tu dominio MAIL FROM personalizado no debe usarse para nada más y cumple los siguientes requisitos:

- El dominio MAIL FROM debe ser un subdominio del dominio principal de una identidad verificada (dirección de correo electrónico o dominio).
- El dominio MAIL FROM no debe ser un subdominio que también utilice para enviar correo electrónico.
- El dominio MAIL FROM no debe ser un subdominio que utilice para recibir correo electrónico.

Uso de SPF con el dominio MAIL FROM personalizado

El marco de directivas de remitente (SPF) es un estándar de validación de correo electrónico que ha sido diseñado para prevenir la suplantación de correo electrónico. Puede configurar el dominio MAIL FROM personalizado con SPF para indicar a los proveedores de correo electrónico qué servidores pueden enviar correo electrónico desde el dominio MAIL FROM personalizado. SPF se define en RFC 7208.

Para configurar un SPF, tiene que publicar un registro TXT en la configuración de DNS del dominio MAIL FROM personalizado. Este registro contiene una lista de los servidores que autoriza a enviar correo electrónico desde el dominio MAIL FROM personalizado. Cuando un proveedor de correo electrónico recibe un mensaje del dominio MAIL FROM personalizado, comprueba los registros DNS del dominio para asegurarse de que el correo electrónico se envió desde un servidor autorizado.

Si desea utilizar este registro SPF como forma de cumplir con DMARC, el dominio de la dirección FROM debe coincidir con el dominio MAIL FROM. Consulte the section called “Conformidad con DMARC a través de SPF”.

En la siguiente sección, the section called “Configuración del dominio MAIL FROM personalizado” explica cómo configurar SPF para el dominio MAIL FROM personalizado.

Configuración del dominio MAIL FROM personalizado

El proceso de configuración de un dominio MAIL FROM personalizado requiere que añada registros a la configuración de DNS del dominio. SES requiere que publiques un registro MX para que tu dominio pueda recibir las notificaciones de devoluciones y quejas que te envíen los proveedores

de correo electrónico. También tiene que publicar un registro SPF (tipo TXT) para demostrar que Amazon SES está autorizado a enviar correo electrónico desde su dominio.

Puedes configurar un dominio MAIL FROM personalizado para todo un dominio o subdominio, así como para direcciones de correo electrónico individuales. Los siguientes procedimientos muestran cómo utilizar la consola de Amazon SES para configurar un dominio MAIL FROM personalizado. También puedes configurar un dominio MAIL FROM personalizado mediante la operación de la API de SetIdentityMailFromdominio.

Configuración de un dominio MAIL FROM personalizado para un dominio verificado

Estos procedimientos le muestran cómo configurar un dominio MAIL FROM personalizado para todo un dominio o subdominio, de modo que todos los mensajes enviados desde las direcciones de ese dominio utilicen este dominio MAIL FROM personalizado.

Para configurar un dominio verificado para que utilice un dominio MAIL FROM personalizado específico

1. Abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación izquierdo, en Configuración, elija Identidades.
3. En la lista de identidades, elija la identidad que desea configurar en la que Identity type (Tipo de identidad) es Domain (Dominio) y Status (Estado) es Verified (Verificado).
    - Si Status (Estado) es Unverified (No verificado), complete los procedimientos indicados en Verificación de una identidad de dominio DKIM con el proveedor de DNS para verificar el dominio de la dirección de correo electrónico.
4. En la parte inferior de la pantalla en el panel Custom MAIL FROM domain (Dominio MAIL FROM personalizado), elija Edit (Editar).
5. En el panel General details (Detalles generales), haga lo siguiente:
    a. Seleccione la casilla de verificación Use a custom MAIL FROM domain (Utilizar un dominio MAIL FROM personalizado).
    b. En MAIL FROM domain, escriba el subdominio que desea utilizar como dominio MAIL FROM.
    c. Para Behavior on MX failure (Comportamiento ante error de MX), elija una de las siguientes opciones:

- Use default MAIL FROM domain (Utilizar dominio MAIL FROM predeterminado): si el registro MX del dominio MAIL FROM personalizado no se ha configurado correctamente, Amazon SES utilizará un subdominio de `amazonses.com`. El subdominio varía en función del lugar en el Región de AWS que utilices Amazon SES.
- Reject message (Rechazar mensaje): si el registro MX del dominio MAIL FROM personalizado no está correctamente configurado, Amazon SES devolverá un error `MailFromDomainNotVerified`. Los mensajes de correo electrónico que intente enviar desde este dominio se rechazarán automáticamente.

d. Elija Save changes (Guardar cambios). Volverá a la pantalla anterior.

6. Publique los registros MX y SPF (tipo TXT) en el servidor DNS del dominio MAIL FROM personalizado:

   En el panel Custom MAIL FROM domain (Dominio MAIL FROM personalizado), la tabla Publish DNS records (Publicar registros DNS) mostrará los registros MX y SPF (tipo TXT) que debe publicar (agregar) a la configuración de DNS del dominio. Estos registros utilizan los formatos que se muestran en la siguiente tabla.

Nombre	Tipo	Valor
subdominio .dominio.com	MX	10 feedback-smtp.*region*.amazonses.com
subdominio .dominio.com	TXT	“v=spf1 include:amazonses.com ~all”

   En los registros anteriores,

   - *subdomain.domain.com* se rellenará con el subdominio MAIL FROM
   - *la región* se rellenará con el nombre de la región Región de AWS en la que desee verificar el dominio MAIL FROM (por ejemplo `us-west-2us-east-1`,, `oeu-west-1`, etc.)
   - El número 10 que aparece junto con el valor MX es el orden de preferencia del servidor de correo y deberá introducirse en un campo de valor independiente según lo especificado por la GUI de su proveedor de DNS.
   - El valor del registro TXT de SPF debe incluir las comillas.

Desde la tabla Publish DNS records (Publicar registros DNS), copie los registros MX y SPF (tipo TXT) eligiendo el icono de copia junto a cada valor y péguelos en los campos correspondientes de la GUI de su proveedor de DNS. También puede elegir Download .csv record set (Descargar el conjunto de registro .csv) para guardar una copia de los registros en su computadora.

> **Important**
>
> Para configurar correctamente un dominio MAIL FROM personalizado con Amazon SES, debe publicar exactamente un registro MX en el servidor DNS de su dominio MAIL FROM. Si el dominio MAIL FROM tiene varios registros MX, la configuración MAIL FROM personalizada con Amazon SES devolverá un error.

Si Route 53 proporciona el servicio DNS para su dominio MAIL FROM y ha iniciado sesión en él AWS Management Console con la misma cuenta que utiliza para Route 53, elija Publicar registros con Route 53. Los registros DNS se aplican automáticamente a la configuración de DNS de su dominio.

Si utiliza otro proveedor de DNS, tendrá que publicar manualmente los registros DNS en el servidor DNS del dominio MAIL FROM. El procedimiento para añadir registros DNS al servidor DNS de su dominio varía en función del servicio de alojamiento web o del proveedor de DNS.

Los procedimientos para publicar los registros de DNS de su dominio dependen del proveedor de DNS utilizado. La tabla que sigue incluye enlaces a la documentación de unos pocos proveedores de DNS muy utilizados. Esta lista no es exhaustiva y no implica aprobación; del mismo modo, si su proveedor de DNS no aparece en la lista, no implica que no admita la configuración de dominio MAIL FROM.

Nombre del proveedor de alojamiento/DNS	Enlace a la documentación
GoDaddy	• MX: Añadir un registro MX (enlace externo) • TXT: Añadir un registro TXT (enlace externo)

Nombre del proveedor de alojamiento/DNS	Enlace a la documentación
DreamHost	• MX: ¿Cómo cambiar mis registros MX? (enlace externo) • TXT: ¿Cómo añadir registros DNS personalizados? (enlace externo)
Cloudflare	• MX: ¿Cómo añadir o editar registros MX o de correo? (enlace externo) • TXT: Administrar registros de DNS en CloudFlare (enlace externo)
HostGator	• MX: Configurar registros de MX (enlace externo) • TXT: administre los registros DNS con HostGator /eNom (enlace externo)
Namecheap	• MX: ¿Cómo configurar los registros MX requeridos para el servicio de correo? (enlace externo) • TXT: ¿Cómo añado registros TXT/SPF/DKIM/DMARC a mi dominio? (enlace externo)
Names.co.uk	• MX: Cambiar la configuración de DNS de su dominio (enlace externo) • TXT: Cambiar la configuración de DNS de su dominio (enlace externo)
Wix	• MX: Añadir o actualizar los registros de MX en su cuenta de Wix (enlace externo) • TXT: Añadir o actualizar registros de TXT en su cuenta de Wix (enlace externo)

Cuando Amazon SES detecta que los registros están en vigor, recibe un correo electrónico informándole de que su dominio MAIL FROM personalizado se ha configurado correctamente.

En función de su proveedor de DNS, es posible que haya un retraso de hasta 72 horas antes de que Amazon SES detecte el registro MX.

Configuración de un dominio MAIL FROM personalizado para una dirección de correo electrónico verificada

También puede configurar un dominio MAIL FROM personalizado para una dirección de correo electrónico específica. Para configurar un dominio MAIL FROM personalizado para una dirección de correo electrónico, debe modificar los registros DNS del dominio al que está asociada la dirección de correo electrónico.

> **Note**
>
> No puede configurar un dominio MAIL FROM personalizado para direcciones de un dominio que no sea de su propiedad (por ejemplo, no puede crear un dominio MAIL FROM personalizado para una dirección del dominio `gmail.com` ya que no puede agregar los registros DNS necesarios al dominio).

Para configurar una dirección de correo electrónico verificada para utilizar un dominio MAIL FROM especificado

1. Abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación izquierdo, en Configuración, selecciona Identidades.
3. En la lista de identidades, elija la identidad que desea configurar en la que Identity type (Tipo de identidad) es Email address (Dirección de correo electrónico) y Status (Estado) es Verified (Verificado).
   - Si Status (Estado) es Unverified (No verificado), complete los procedimientos indicados en Verificación de una identidad de dirección de correo electrónico para verificar el dominio de la dirección de correo electrónico.
4. En la pestaña MAIL FROM Dominio (Dominio MAIL FROM), elija Edit (Editar) en el panel Custom MAIL FROM domain (Dominio MAIL FROM personalizado).
5. En el panel General details (Detalles generales), haga lo siguiente:
   a. Seleccione la casilla de verificación Use a custom MAIL FROM domain (Utilizar un dominio MAIL FROM personalizado).

b. En MAIL FROM domain, escriba el subdominio que desea utilizar como dominio MAIL FROM.

c. Para Behavior on MX failure (Comportamiento ante error de MX), elija una de las siguientes opciones:

- Use default MAIL FROM domain (Utilizar dominio MAIL FROM predeterminado): si el registro MX del dominio MAIL FROM personalizado no se ha configurado correctamente, Amazon SES utilizará un subdominio de `amazonses.com`. El subdominio varía en función del lugar en el Región de AWS que utilices Amazon SES.
- Reject message (Rechazar mensaje): si el registro MX del dominio MAIL FROM personalizado no está correctamente configurado, Amazon SES devolverá un error `MailFromDomainNotVerified`. Los mensajes de correo electrónico que intente enviar desde esta dirección se rechazarán automáticamente.

d. Elija Save changes (Guardar cambios). Volverá a la pantalla anterior.

6. Publique los registros MX y SPF (tipo TXT) en el servidor DNS del dominio MAIL FROM personalizado:

   En el panel Custom MAIL FROM domain (Dominio MAIL FROM personalizado), la tabla Publish DNS records (Publicar registros DNS) mostrará los registros MX y SPF (tipo TXT) que debe publicar (agregar) a la configuración de DNS del dominio. Estos registros utilizan los formatos que se muestran en la siguiente tabla.

Nombre	Tipo	Valor
subdominio .dominio.com	MX	10 feedback-smtp.*region*.amazonses.com
subdominio .dominio.com	TXT	“v=spf1 include:amazonses.com ~all”

   En los registros anteriores,

- *subdomain*.*domain*.*com* se rellenará con el subdominio MAIL FROM
- *la región* se rellenará con el nombre de la región Región de AWS en la que desee verificar el dominio MAIL FROM (por ejemplo `us-west-2us-east-1`,, `oeu-west-1`, etc.)

- El número 10 que aparece junto con el valor MX es el orden de preferencia del servidor de correo y deberá introducirse en un campo de valor independiente según lo especificado por la GUI de su proveedor de DNS.
- El valor del registro TXT de SPF debe incluir las comillas.

Desde la tabla Publish DNS records (Publicar registros DNS), copie los registros MX y SPF (tipo TXT) eligiendo el icono de copia junto a cada valor y péguelos en los campos correspondientes de la GUI de su proveedor de DNS. También puede elegir Download .csv record set (Descargar el conjunto de registro .csv) para guardar una copia de los registros en su computadora.

> **Important**
>
> Para configurar correctamente un dominio MAIL FROM personalizado con Amazon SES, debe publicar exactamente un registro MX en el servidor DNS de su dominio MAIL FROM. Si el dominio MAIL FROM tiene varios registros MX, la configuración MAIL FROM personalizada con Amazon SES devolverá un error.

Si Route 53 proporciona el servicio DNS para su dominio MAIL FROM y ha iniciado sesión en él AWS Management Console con la misma cuenta que utiliza para Route 53, elija Publicar registros con Route 53. Los registros DNS se aplican automáticamente a la configuración de DNS de su dominio.

Si utiliza otro proveedor de DNS, tendrá que publicar manualmente los registros DNS en el servidor DNS del dominio MAIL FROM. El procedimiento para añadir registros DNS al servidor DNS de su dominio varía en función del servicio de alojamiento web o del proveedor de DNS.

Los procedimientos para publicar los registros de DNS de su dominio dependen del proveedor de DNS utilizado. La tabla que sigue incluye enlaces a la documentación de unos pocos proveedores de DNS muy utilizados. Esta lista no es exhaustiva y no implica aprobación; del mismo modo, si su proveedor de DNS no aparece en la lista, no implica que no admita la configuración de dominio MAIL FROM.

Nombre del proveedor de alojamiento/DNS	Enlace a la documentación
GoDaddy	• MX: Añadir un registro MX (enlace externo) • TXT: Añadir un registro TXT (enlace externo)
DreamHost	• MX: ¿Cómo cambiar mis registros MX? (enlace externo) • TXT: ¿Cómo añadir registros DNS personalizados? (enlace externo)
Cloudflare	• MX: ¿Cómo añadir o editar registros MX o de correo? (enlace externo) • TXT: Administrar registros de DNS en CloudFlare (enlace externo)
HostGator	• MX: Cambiar registros MX - Windows (enlace externo) • TXT: administre los registros DNS con HostGator /eNom (enlace externo)
Namecheap	• MX: ¿Cómo configurar los registros MX requeridos para el servicio de correo? (enlace externo) • TXT: ¿Cómo añado registros TXT/SPF/DKIM/DMARC a mi dominio? (enlace externo)
Names.co.uk	• MX: Cambiar la configuración de DNS de su dominio (enlace externo) • TXT: Cambiar la configuración de DNS de su dominio (enlace externo)

Nombre del proveedor de alojamiento/DNS	Enlace a la documentación
Wix	• MX: Añadir o actualizar los registros de MX en su cuenta de Wix (enlace externo) • TXT: Añadir o actualizar registros de TXT en su cuenta de Wix (enlace externo)

Cuando Amazon SES detecta que los registros están en vigor, recibe un correo electrónico informándole de que su dominio MAIL FROM personalizado se ha configurado correctamente. En función de su proveedor de DNS, es posible que haya un retraso de hasta 72 horas antes de que Amazon SES detecte el registro MX.

Estados de configuración de dominio MAIL FROM personalizado con Amazon SES

Después de configurar una identidad para utilizar un dominio MAIL FROM personalizado, el estado de la configuración es “pending” (pendiente) mientras Amazon SES intenta detectar el registro MX necesarios en su configuración de DNS. El estado cambia a continuación, en función de si Amazon SES detecta el registro MX. En la siguiente tabla se describen los comportamientos de envío de correo electrónico y las acciones de Amazon SES asociadas a cada estado. Cada vez que el estado cambia, Amazon SES envía una notificación a la dirección de correo electrónico asociada a su Cuenta de AWS.

Estado	Comportamiento de envío de correo electrónico	Acciones de Amazon SES
Pendiente	Utiliza una configuración alternativa de MAIL FROM personalizada	Amazon SES intenta detectar el registro MX necesario durante 72 horas. Si no tiene éxito, el estado cambia a "Failed".

Estado	Comportamiento de envío de correo electrónico	Acciones de Amazon SES
Success	Utiliza dominio MAIL FROM personalizado	Amazon SES comprueba continuamente que el registro MX está en vigor.
Temporary Failure	Utiliza una configuración alternativa de MAIL FROM personalizada	Amazon SES intenta detectar el registro MX necesario durante 72 horas. Si no tiene éxito, el estado cambia a "Failed"; en caso de éxito, el estado cambia a "Success".

Estado	Comportamiento de envío de correo electrónico	Acciones de Amazon SES
Con error	Utiliza una configuración alternativa de MAIL FROM personalizada	Amazon SES ya no intenta detectar el registro MX necesario. Para utilizar un dominio MAIL FROM personalizado, debe reiniciar el proceso de configuración en Configuración del dominio MAIL FROM personalizado.

Cumplimiento del protocolo de autenticación DMARC en Amazon SES

La autenticación, la presentación de informes y la conformidad de los mensajes basados en el dominio (DMARC) es un protocolo de autenticación de correo electrónico que utiliza el Sender Policy Framework (SPF) y el correo DomainKeys identificado (DKIM) para detectar la suplantación de identidad y la suplantación de identidad del correo electrónico. Para cumplir con el DMARC, los mensajes deben autenticarse mediante el SPF o el DKIM, pero lo ideal es que, cuando se utilicen ambos con el DMARC, se garantice el mayor nivel de protección posible para el envío de correos electrónicos.

Repasemos brevemente lo que hace cada uno de ellos y cómo el DMARC los une a todos:

- SPF: identifica qué servidores de correo están autorizados a enviar correo en nombre de tu dominio MAIL FROM personalizado mediante un registro TXT de DNS que utiliza DNS. Los sistemas de correo de los destinatarios utilizan el registro TXT del SPF para determinar si un mensaje de su dominio personalizado proviene de un servidor de mensajería autorizado. Básicamente, el SPF está diseñado para ayudar a prevenir la suplantación de identidad, pero

existen técnicas de suplantación de identidad a las que el SPF es susceptible en la práctica, por lo que es necesario utilizar también el DKIM junto con el DMARC.

- DKIM: añade una firma digital a los mensajes salientes en el encabezado del correo electrónico. Los sistemas de recepción de correo electrónico pueden usar esta firma digital para comprobar si el correo entrante está firmado por una clave propiedad del dominio. Sin embargo, cuando un sistema de correo electrónico receptor reenvía un mensaje, el sobre del mensaje se cambia de forma que se invalida la autenticación SPF. Como la firma digital permanece en el mensaje de correo electrónico porque forma parte del encabezado del correo electrónico, el DKIM funciona incluso cuando un mensaje se ha reenviado entre servidores de correo (siempre y cuando el contenido del mensaje no se haya modificado).
- DMARC: garantiza que el dominio esté alineado con al menos uno de los dominios SPF y DKIM. El uso exclusivo de SPF y DKIM no garantiza que la dirección de origen esté autenticada (es la dirección de correo electrónico que el destinatario ve en su cliente de correo electrónico). El SPF solo comprueba el dominio especificado en la dirección MAIL FROM (que el destinatario no ve). El DKIM solo comprueba el dominio especificado en la firma del DKIM (además, el destinatario no lo ve). El DMARC resuelve estos dos problemas al exigir que la alineación de los dominios sea correcta en el SPF o en el DKIM:
  - Para que el SPF supere la alineación con el DMARC, el dominio de la dirección de origen debe coincidir con el dominio de la dirección MAIL FROM (también denominada ruta de devolución y dirección de origen del paquete). Esto rara vez es posible con el correo reenviado, ya que se elimina, o cuando se envía correo a través de proveedores de correo masivo externos, ya que la ruta de devolución (MAIL FROM) se utiliza para los rebotes y las quejas que el proveedor (SES) rastrea con una dirección de su propiedad.
  - Para que el DKIM supere la alineación DMARC, el dominio especificado en la firma del DKIM debe coincidir con el dominio de la dirección de origen. Si utilizas remitentes o servicios de terceros que envían correo en tu nombre, asegúrate de que el remitente externo esté correctamente configurado para la firma DKIM y de que hayas agregado los registros DNS correspondientes en tu dominio. Los servidores de correo receptores podrán entonces verificar el correo que les haya enviado un tercero como si lo hubiera enviado una persona autorizada a usar una dirección del dominio.

Combinándolo todo con DMARC

Las comprobaciones de alineación de los DMARC que analizamos anteriormente muestran cómo el SPF, el DKIM y el DMARC trabajan juntos para aumentar la confianza en su dominio y la entrega de

sus correos electrónicos a las bandejas de entrada. Para ello, DMARC garantiza que la dirección de origen que ve el destinatario esté autenticada por SPF o DKIM:

- Un mensaje pasa por el DMARC si se aprueba una o las dos comprobaciones de SPF o DKIM descritas.
- Un mensaje no supera el DMARC si fallan las dos comprobaciones de SPF o DKIM descritas.

Por lo tanto, tanto el SPF como el DKIM son necesarios para que DMARC tenga la mejor oportunidad de autenticar el correo electrónico enviado y, al utilizar los tres, ayudará a garantizar que tiene un dominio de envío totalmente protegido.

DMARC también te permite indicar a los servidores de correo electrónico cómo gestionar los correos electrónicos cuando no cumplen con la autenticación DMARC mediante las políticas que tú establezcas. Esto se explicará en la siguiente secciónthe section called “Configuración de la política de DMARC en un dominio”, que contiene información sobre cómo configurar sus dominios de SES para que los correos electrónicos que envíe cumplan con el protocolo de autenticación DMARC mediante el SPF y el DKIM.

Configuración de la política de DMARC en un dominio

Para configurar DMARC, es necesario modificar la configuración de DNS del dominio. La configuración de DNS del dominio debe incluir un registro TXT que especifique la configuración de DMARC del dominio. Los procedimientos para añadir registros TXT a la configuración de DNS dependen del proveedor de DNS o de alojamiento que utilice. Si utiliza Route 53, consulte Trabajar con registros en la Guía para desarrolladores de Amazon Route 53. Si utiliza otro proveedor, consulte la documentación de configuración de DNS correspondiente.

El nombre del registro TXT que cree debe ser `_dmarc.`*`example.com`*, donde *`example.com`* es el dominio. El valor del registro TXT contiene la política de DMARC que se aplica al dominio. A continuación, se muestra un ejemplo de un registro TXT que contiene una política de DMARC:

Nombre	Tipo	Valor
`_dmarc.example.com`	TXT	`"v=DMARC1;p=quarantine;rua=mailto:my_dmarc_report@example.com"`

En el ejemplo anterior de política de DMARC, esta política indica a los proveedores de correo electrónico que hagan lo siguiente:

- En el caso de los mensajes que no se puedan autenticar, envíelos a la carpeta de correo no deseado según lo especificado en el parámetro de política,`p=quarantine`. Otras opciones incluyen no hacer nada mediante `p=none` el uso o rechazar el mensaje directamente mediante el uso de. `p=reject`
  - En la siguiente sección se explica cómo y cuándo utilizar estas tres configuraciones de política. Si se utiliza una configuración incorrecta en el momento incorrecto, puede provocar que el correo electrónico no se entregue, consulte. the section called “Implementación de DMARC”
- Envíe informes sobre todos los correos electrónicos que no se hayan autenticado correctamente en un resumen (es decir, un informe que agrupe los datos de un período de tiempo determinado, en lugar de enviar informes individuales para cada evento) según lo especifique el parámetro de informe `rua=mailto:my_dmarc_report@example.com` (rua significa URI de informes agregados). Normalmente, los proveedores de correo electrónico envían estos informes agregados una vez al día, aunque estas políticas difieren de un proveedor a otro.

Para obtener más información sobre la configuración de DMARC en el dominio, consulte la página Overview en el sitio web de DMARC.

Para ver las especificaciones completas del sistema DMARC, consulte el borrador del DMARC del Grupo de Trabajo de Ingeniería de Internet (IETF).

Mejores prácticas para implementar el DMARC

Lo mejor es implementar la aplicación de las políticas de DMARC de forma gradual y gradual para que no interrumpa el resto del flujo de correo. Cree e implemente un plan de implementación que siga estos pasos. Realice cada uno de estos pasos primero con cada uno de sus subdominios y, finalmente, con el dominio de nivel superior de su organización antes de pasar al siguiente paso.

1. Supervise el impacto de la implementación de DMARC (p=none).
   - Comience con un registro sencillo en modo de supervisión para un subdominio o dominio en el que se solicite que las organizaciones receptoras de correo le envíen estadísticas sobre los mensajes que vean utilizando ese dominio. Un registro en modo de supervisión es un registro TXT de DMARC cuya política está establecida en none. `p=none`
   - Los informes generados a través del DMARC indicarán los números y las fuentes de los mensajes que superen estas comprobaciones, en comparación con los que no. Puedes ver

fácilmente qué parte de tu tráfico legítimo está cubierto o no por ellos. Verás señales de reenvío, ya que los mensajes reenviados no superarán el SPF y el DKIM si se modifica el contenido. También empezarás a ver cuántos mensajes fraudulentos se están enviando y desde dónde se envían.

- Los objetivos de este paso son saber qué correos electrónicos se verán afectados al implementar uno de los dos pasos siguientes y lograr que cualquier tercero o remitente autorizado armonice sus políticas de SPF o DKIM.
- Lo mejor para los dominios existentes.

2. Solicita que los sistemas de correo externos pongan en cuarentena el correo que no supere el DMARC (p=quarantine).
   - Si cree que todo o la mayor parte de su tráfico legítimo se envía a dominios alineados con el SPF o el DKIM, y comprende el impacto de la implementación del DMARC, puede implementar una política de cuarentena. Una política de cuarentena es un registro TXT de DMARC cuya política está configurada como puesta en cuarentena. `p=quarantine` De este modo, pides a los receptores de DMARC que coloquen los mensajes de tu dominio que no superen el DMARC en el equivalente local de una carpeta de correo no deseado en lugar de en las bandejas de entrada de tus clientes.
   - Ideal para dominios en transición que han analizado los informes de DMARC durante el paso 1.
3. Solicita que los sistemas de correo externos no acepten mensajes que no superen el DMARC (p=reject).
   - La implementación de una política de rechazo suele ser el último paso. Una política de rechazo es un registro TXT de DMARC cuya política está configurada para rechazarp=`reject`. Al hacerlo, se pide a los receptores de DMARC que no acepten los mensajes que no pasen las comprobaciones de DMARC, lo que significa que ni siquiera se pondrán en cuarentena en una carpeta de correo no deseado o basura, sino que se rechazarán de plano.
   - Si utilizas una política de rechazo, sabrás exactamente qué mensajes no cumplen con la política de DMARC, ya que el rechazo provocará un rebote del SMTP. Con la cuarentena, los datos agregados proporcionan información sobre los porcentajes de correos electrónicos que pasan o no superan las comprobaciones de SPF, DKIM y DMARC.
   - Ideal para dominios nuevos o dominios existentes que hayan pasado por los dos pasos anteriores.

Conformidad con DMARC a través de SPF

Para que un correo electrónico cumpla los requisitos de DMARC basado en SPF, se deben cumplir estas dos condiciones:

- El mensaje debe pasar una comprobación SPF, ya que dispone de un registro SPF (tipo TXT) válido que hayas publicado en la configuración DNS de tu dominio MAIL FROM personalizado.
- El dominio de la dirección de origen del encabezado del correo electrónico debe alinearse (coincidir) con el dominio, o un subdominio, especificado en la dirección de origen. Para lograr la alineación del SPF con el SES, la política de DMARC del dominio no debe especificar una política de SPF estricta (aspf=s).

Para cumplir estos requisitos, siga los pasos que se describen a continuación:

- Configure un dominio MAIL FROM personalizado realizando los procedimientos que se describen en the section called “Uso de un dominio MAIL FROM personalizado”.
- Asegúrese de que el dominio de envío use una política laxa para SPF. Si no has cambiado la alineación de las políticas de tu dominio, este utilizará una política más flexible de forma predeterminada, al igual que SES.

> **Note**
>
> Puede determinar la conformidad con DMARC para SPF del dominio escribiendo el siguiente comando en la línea de comandos y reemplazando *example.com* por su dominio:
>
> ```
> dig -type=TXT _dmarc.example.com
> ```
>
> En el resultado de este comando, bajo Non-authoritative answer, busque un registro que empiece por `v=DMARC1`. Si este registro incluye la cadena `aspf=r` o si la cadena `aspf` no aparece, entonces el dominio usa la conformidad laxa para SPF. Si el registro incluye la cadena `aspf=s`, entonces el dominio usa la conformidad estricta para SPF. El administrador del sistema tendrá que eliminar esta etiqueta del registro TXT DMARC en la configuración de DNS del dominio.
> Como alternativa, puede utilizar una herramienta de búsqueda de DMARC basada en la web, como el Inspector de DMARC del sitio web de dmarcian o la herramienta de

verificación de DMARC del sitio MxToolBox web, para determinar la alineación de las políticas de su dominio con respecto al SPF.

Conformidad con DMARC a través de DKIM

Para que un correo electrónico cumpla los requisitos de DMARC basado en DKIM, se deben cumplir estas dos condiciones:

- El mensaje debe tener una firma DKIM válida y superar la comprobación de DKIM.
- El dominio especificado en la firma DKIM debe alinearse (coincidir) con el dominio de la dirección de origen. Si la política de DMARC del dominio especifica una alineación estricta para el DKIM, estos dominios deben coincidir exactamente (SES usa una política de DKIM estricta de forma predeterminada).

Para cumplir estos requisitos, siga los pasos que se describen a continuación:

- Configure Easy DKIM realizando los procedimientos que se describen en the section called “Easy DKIM”. Cuando se utiliza Easy DKIM, Amazon SES firma automáticamente los mensajes de correo electrónico.

  > **Note**
  >
  > En lugar de utilizar Easy DKIM, también puede firmar manualmente sus mensajes. Sin embargo, en tal caso, debe tener cuidado, ya que Amazon SES no valida la firma DKIM que usted crea. Por este motivo, le recomendamos que utilice Easy DKIM.

- Asegúrese de que el dominio especificado en la firma DKIM esté alineado con el dominio de la dirección de origen. O bien, si lo envía desde un subdominio del dominio en la dirección de origen, asegúrese de que su política de DMARC esté configurada de manera flexible.

  > **Note**
  >
  > Puede determinar la conformidad con DMARC para DKIM del dominio escribiendo el siguiente comando en la línea de comandos y reemplazando *example.com* por su dominio:
  >
  > ```
  > dig -type=TXT _dmarc.example.com
  > ```

En el resultado de este comando, bajo Non-authoritative answer, busque un registro que empiece por `v=DMARC1`. Si este registro incluye la cadena `adkim=r` o si la cadena `adkim` no aparece, entonces el dominio usa la conformidad laxa para DKIM. Si el registro incluye la cadena `adkim=s`, entonces el dominio usa la conformidad estricta para DKIM. El administrador del sistema tendrá que eliminar esta etiqueta del registro TXT DMARC en la configuración de DNS del dominio.
Como alternativa, puede utilizar una herramienta de búsqueda de DMARC basada en la web, como el Inspector de DMARC del sitio web de dmarcian o la herramienta de verificación de DMARC del sitio MxToolBox web, para determinar la alineación de las políticas de su dominio con respecto al DKIM.

Uso de BIMI en Amazon SES

Los indicadores de marca para la identificación de mensajes (BIMI) son una especificación de correo electrónico que permite que las bandejas de entrada de correo electrónico muestren el logotipo de una marca junto a los mensajes de correo electrónico autenticados de la marca en los clientes de correo electrónico compatibles.

BIMI es una especificación de correo electrónico que se conecta directamente a la autenticación, pero no es un protocolo de autenticación de correo electrónico independiente, ya que requiere que todo el correo electrónico cumpla con la autenticación DMARC.

Aunque BIMI requiere DMARC, DMARC requiere que el dominio tenga registros SPF o DKIM para alinearlos, pero es mejor incluir registros SPF y DKIM para mayor seguridad y porque algunos proveedores de servicios de correo electrónico (ESP) requieren ambos cuando utilizan BIMI. En la siguiente sección se describen los pasos para implementar BIMI en Amazon SES.

Configuración de BIMI en SES

Puede configurar BIMI para un dominio de correo electrónico que posea; en SES, se denomina dominio MAIL FROM personalizado. Una vez configurados, todos los mensajes que envíe desde ese dominio mostrarán el logotipo de BIMI en clientes de correo electrónico compatibles con BIMI.

Para permitir que los correos electrónicos muestren un logotipo de BIMI, es necesario cumplir algunos requisitos previos en SES. En el siguiente procedimiento, estos requisitos previos se generalizan y harán referencia a secciones específicas que abordan estos temas en detalle. Los pasos específicos de BIMI y lo que se necesita para configurarlo en SES se detallarán aquí.

Para configurar BIMI en un dominio MAIL FROM personalizado

1. Debe tener un dominio MAIL FROM personalizado configurado en SES con registros SPF (tipo TXT) y MX publicados para ese dominio. Si todavía no tiene un dominio MAIL FROM personalizado o desea crear uno nuevo para el logotipo de BIMI, consulte the section called “Uso de un dominio MAIL FROM personalizado”.
2. Configure el dominio con Easy DKIM. Consulte the section called “Easy DKIM”.
3. Configure el dominio con DMARC publicando un registro TXT con el proveedor de DNS con las siguientes especificaciones de política de cumplimiento necesarias para BIMI:

Nombre	Tipo	Valor
`_dmarc.example.com`	`TXT`	`v=DMARC1;p=quarantine;pct=100;rua=mailto:dmarcreports@example.com`
		`v=DMARC1;p=reject;rua=mailto:dmarcreports@example.com`

   En el ejemplo de política DMARC anterior, tal como se requiere para BIMI:

   - *`example.com`* se debe sustituir por el nombre de dominio o subdominio.
   - El valor p= puede ser:
     - poner en cuarentena con un valor pct establecido en 100, como se muestra, o
     - rechazar como se muestra.
   - Si envía desde un subdominio, BIMI exige que el dominio principal también cuente con esta política de cumplimiento. Los subdominios se regirán por la política del dominio principal. Sin embargo, si agrega un registro de DMARC para el subdominio además del que se publica para el dominio principal, el subdominio también debe tener la misma política de cumplimiento para ser elegible para BIMI.
   - Si nunca ha configurado una política de DMARC para el dominio, consulte the section called “Autenticación de correo electrónico con DMARC” y asegúrese de que solo usa los valores de la política de DMARC específicos de BIMI, tal como se muestra.
4. Cree el logotipo de BIMI como un archivo `.svg` de gráficos vectoriales escalables (SVG); el perfil SVG específico que requiere BIMI se define como SVG Portable/Secure (SVG P/S). Para

que el logotipo se muestre en el cliente de correo electrónico, debe cumplir exactamente con estas especificaciones. Consulte la guía del Grupo de BIMI sobre la creación de archivos de logotipos SVG y las herramientas de conversión SVG recomendadas.

5. (Opcional) Obtenga un certificado de marca verificada (VMC). Algunos ESP, como Gmail y Apple, exigen que un VMC demuestre que es el propietario de la marca comercial y el contenido del logotipo de BIMI. Si bien esto no es un requisito para implementar el BIMI en el dominio, el logotipo de BIMI no se mostrará en el cliente de correo electrónico si el ESP al que envíe el correo cumple con el VMC. Consulte las referencias del Grupo de BIMI a las autoridades de certificación participantes para obtener un VMC para el logotipo.
6. Aloje el archivo SVG del logotipo de BIMI en un servidor al que tenga acceso para que sea accesible públicamente a través de HTTPS. Por ejemplo, puede cargarlo en un bucket de Amazon S3.
7. Cree y publique un registro de DNS de BIMI que incluya una URL para el logotipo. Cuando un ESP compatible con BIMI compruebe el registro de DMARC, también buscará un registro de BIMI que contenga la URL del archivo `.svg` del logotipo y, si está configurado, la URL del archivo `.pem` de VMC. Si los registros coinciden, mostrarán el logotipo de BIMI.

   Configure el dominio con BIMI publicando un registro TXT con el proveedor de DNS con los siguientes valores, tal como se muestra: el envío desde un dominio se representa en el primer ejemplo; el envío desde un subdominio se representa en el segundo ejemplo:

Nombre	Tipo	Valor
`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`		

   En los ejemplos de registros de BIMI anteriores:

   - El valor del nombre se debe especificar literalmente `default._bimi.` como un subdominio de *`example.com`* o *`marketing.example.com`* que se debe sustituir por el nombre de dominio o subdominio.
   - El valor `v=` es la versión del registro de BIMI.

- El valor `l=` es el logotipo que representa la URL que apunta al archivo `.svg` de la imagen.
- El valor `a=` es la autoridad que representa la URL que apunta al archivo `.pem` del certificado.

Puede validar el registro de BIMI con una herramienta como el Inspector de BIMI del grupo de BIMI.

El último paso de este proceso es tener un patrón de envío regular a los ESP que admitan la colocación del logotipo de BIMI. El dominio debe tener una cadencia de entrega regular y debe tener una buena reputación entre los ESP a los que envía. La colocación del logotipo de BIMI puede tardar en llegar a los ESP en los que no tenga una reputación o una cadencia de envío establecidos.

Puede encontrar más información y recursos relacionados con el BIMI a través de la organización del Grupo de BIMI.

Configuración de las notificaciones de eventos para Amazon SES

Para poder enviar correo electrónico con Amazon SES, debe disponer de un sistema para administrar los rebotes y los reclamos. Amazon SES puede informarle de eventos de rebotes o reclamos de tres maneras: mediante el envío de un correo electrónico de notificación, con la notificación de un tema de Amazon SNS o con la publicación de eventos de envío. Esta sección contiene información acerca de cómo configurar Amazon SES para enviar determinados tipos de notificaciones, bien por correo electrónico, bien mediante la notificación a un tema de Amazon SNS. Para obtener más información sobre cómo publicar eventos de envío, consulte Monitoreo del envío de correo electrónico mediante la publicación de eventos de Amazon SES.

Puede configurar notificaciones utilizando la consola de Amazon SES o la API de Amazon SES.

Temas

- Consideraciones importantes
- Recepción de notificaciones de Amazon SES por correo electrónico
- Recepción de notificaciones de Amazon SES mediante Amazon SNS

Consideraciones importantes

Hay que tener en cuenta varios puntos importantes al configurar Amazon SES para enviar notificaciones:

- Las notificaciones de correo electrónico y de Amazon SNS se aplican a identidades individuales (las direcciones de correo electrónico o los dominios verificados que se utilizan para enviar correo electrónico). Cuando se habilitan las notificaciones para una identidad, Amazon SES solo envía notificaciones para los mensajes de correo electrónico enviados desde dicha identidad, y únicamente en la región de AWS en la que se hayan configurado las notificaciones.
- Es necesario habilitar un método de recepción de notificaciones de rebotes o reclamaciones. Puede enviar notificaciones al dominio o a la dirección de correo electrónico que generó el rebote o el reclamo, o a un tema de Amazon SNS. También puedes usar la publicación de eventos para enviar notificaciones sobre distintos tipos de eventos (incluidos rebotes, quejas, entregas y más) a un tema de Amazon SNS o a una transmisión de Firehose.

  Si no se configura uno de estos métodos de recepción de notificaciones de rebotes y reclamos, Amazon SES reenvía automáticamente las notificaciones de rebotes y reclamos a la dirección Return-Path (o la dirección Source, si no se ha especificado una dirección Return-Path) del mensaje que generó el evento de rebote o de reclamo, aunque se haya desactivado el reenvío de retroalimentación de correo electrónico.

  Si deshabilita el reenvío de retroalimentación de correo electrónico y habilita la publicación de eventos, debe aplicar el conjunto de configuración que contiene la regla de publicación de eventos a todos los mensajes de correo electrónico que envíe. En esta situación, si no se utiliza el conjunto de configuración, Amazon SES reenvía automáticamente las notificaciones de rebotes y reclamos a la dirección Return-Path o Source del correo electrónico que generó el evento de rebote o reclamo.
- Si configura Amazon SES para enviar eventos de rebotes y reclamos utilizando varios métodos (como, por ejemplo, mediante el envío de notificaciones de correo electrónico o el uso de eventos de envío), es posible que reciba más de una notificación para el mismo evento.

Recepción de notificaciones de Amazon SES por correo electrónico

Amazon SES puede enviarle correo electrónico cuando reciba rebotes y reclamos mediante un proceso denominado reenvío de retroalimentación de correo electrónico.

Para poder enviar correo electrónico con Amazon SES, debe configurarlo para enviar las notificaciones de rebotes y reclamos mediante uno de los siguientes métodos:

- Habilitando el reenvío de retroalimentación de correo electrónico. El procedimiento para configurar este tipo de notificación se incluye en esta sección.

- Enviando notificaciones a un tema de Amazon SNS. Para obtener más información, consulte Recepción de notificaciones de Amazon SES mediante Amazon SNS.
- Publicando notificaciones de eventos. Para obtener más información, consulte Monitoreo del envío de correo electrónico mediante la publicación de eventos de Amazon SES.

> **Important**
>
> Para conocer varios puntos importantes acerca de las notificaciones, consulte Configuración de las notificaciones de eventos para Amazon SES.

Temas

- Habilitar el reenvío de retroalimentación de correo electrónico
- Deshabilitar el reenvío de retroalimentación de correo electrónico
- Destino de reenvío de retroalimentación de correo electrónico

Habilitar el reenvío de retroalimentación de correo electrónico

El reenvío de retroalimentación de correo electrónico está habilitado de forma predeterminada. Si anteriormente lo deshabilitó, puede habilitarlo siguiendo los procedimientos de esta sección.

Para habilitar el reenvío de rebotes y reclamos a través de correo electrónico utilizando la consola de Amazon SES

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).
3. En la lista de direcciones de correo electrónico o dominios verificados, elija la dirección de correo electrónico o el dominio en los que desea configurar las notificaciones de rebotes y reclamaciones.
4. En el panel de detalles de la derecha, expanda la sección Notifications.
5. Elija Edit Configuration.
6. En Email Feedback Forwarding, elija Enabled.

> **Note**
>
> Los cambios que realice en esta página pueden tardar varios minutos en surtir efecto.

También puedes habilitar las notificaciones de devoluciones y quejas por correo electrónico mediante la operación de SetIdentityFeedbackForwardingEnabledAPI.

Deshabilitar el reenvío de retroalimentación de correo electrónico

Si configura un método diferente para proporcionar notificaciones de rebotes y reclamaciones, puede deshabilitar el reenvío de retroalimentación de correo electrónico para no recibir varias notificaciones cuando se produzca un evento de rebote o reclamación.

Para desactivar el reenvío de rebotes y reclamos a través de correo electrónico utilizando la consola de Amazon SES

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).
3. En la lista de direcciones de correo electrónico o dominios verificados, elija la dirección de correo electrónico o el dominio en los que desea configurar las notificaciones de rebotes y reclamaciones.
4. En el panel de detalles de la derecha, expanda la sección Notifications.
5. Elija Edit Configuration.
6. En Email Feedback Forwarding, elija Disabled.

> **Note**
>
> Debe configurar un método de recepción de notificaciones de rebotes y reclamos para poder enviar correo electrónico a través de Amazon SES. Si inhabilitas el reenvío de comentarios por correo electrónico, debes habilitar las notificaciones enviadas por Amazon SNS o publicar los eventos de rebote y queja en un tema de Amazon SNS o en una transmisión de Firehose mediante la publicación de eventos. Si utiliza la publicación de eventos, debe aplicar también el conjunto de configuración que contiene la regla de publicación de eventos a cada mensaje de correo electrónico que envíe. Si no se

configura un método de recepción de notificaciones de rebotes y reclamos, Amazon SES reenvía automáticamente las notificaciones de retroalimentación por correo electrónico a las direcciones que figuran en el campo Return-Path (o en el campo Source, si no se ha especificado una dirección Return-Path) del mensaje que generó el evento de rebote o de reclamo. En esta situación, Amazon SES reenvía las notificaciones de rebotes y reclamos incluso si se han desactivado las notificaciones de retroalimentación de correo electrónico.

7. Para guardar su configuración de notificaciones, elija Save Config (Guardar configuración).

> **Note**
>
> Los cambios que realice en esta página podrían tardar varios minutos en surtir efecto.

También puedes desactivar las notificaciones de rebote y quejas por correo electrónico mediante la operación de la API. SetIdentityFeedbackForwardingEnabled

Destino de reenvío de retroalimentación de correo electrónico

Al recibir notificaciones por correo electrónico, Amazon SES vuelve a escribir el encabezado `From` y le envía la notificación. La dirección a la que Amazon SES reenvía la notificación depende de cómo haya enviado el mensaje original.

Si ha utilizado la interfaz de SMTP para enviar el mensaje, las notificaciones se entregan de acuerdo con las siguientes normas:

- Si ha especificado un encabezado `Return-Path` en la sección `SMTP DATA`, las notificaciones se envían a esa dirección.
- De lo contrario, las notificaciones se envían a la dirección que especificó al ejecutar el comando MAIL FROM.

Si ha utilizado la operación de la API `SendEmail` para enviar el mensaje, las notificaciones se entregan de acuerdo con las siguientes reglas:

- Si ha especificado el parámetro `ReturnPath` opcional en la llamada a la API `SendEmail`, las notificaciones se envían a esa dirección.

- De lo contrario, las notificaciones se envían a la dirección especificada en el parámetro `Source` obligatorio de `SendEmail`.

Si ha utilizado la operación de la API `SendRawEmail` para enviar el mensaje, las notificaciones se entregan de acuerdo con las siguientes reglas:

- Si ha especificado un encabezado `Return-Path` en el mensaje sin procesar, las notificaciones se envían a esa dirección.
- Sin embargo, si ha especificado un parámetro `Source` en la llamada a la API `SendRawEmail`, las notificaciones se envían a esa dirección.
- De lo contrario, las notificaciones se envían a la dirección del encabezado `From` del mensaje sin procesar.

> **Note**
>
> Cuando se especifica una dirección `Return-Path` en un mensaje de correo electrónico, las notificaciones se reciben en esa dirección. Sin embargo, la versión del mensaje que recibe el destinatario contiene un encabezado `Return-Path` que incluye una dirección de correo electrónico anónima (como a0b1c2d3e4f5a6b7-c8d9e0f1-a2b3-c4d5-e6f7-a8b9c0d1e2f3-000000@amazonses.com). Esta dirección anónima se utiliza independientemente de la forma en que se haya enviado el correo electrónico.

Recepción de notificaciones de Amazon SES mediante Amazon SNS

Puede configurar Amazon SES para notificar a un tema de Amazon SNS cuando se reciban rebotes o reclamos, o cuando se entreguen mensajes de correo electrónico. Las notificaciones de Amazon SNS están en formato JavaScript Object Notation (JSON), lo que le permite procesarlas mediante programación.

Para poder enviar correo electrónico con Amazon SES, debe configurarlo para enviar las notificaciones de rebotes y reclamos mediante uno de los siguientes métodos:

- Enviando notificaciones a un tema de Amazon SNS. El procedimiento para configurar este tipo de notificación se incluye en esta sección.
- Habilitando el reenvío de retroalimentación de correo electrónico. Para obtener más información, consulte Recepción de notificaciones de Amazon SES por correo electrónico.

- Publicando notificaciones de eventos. Para obtener más información, consulte Monitoreo del envío de correo electrónico mediante la publicación de eventos de Amazon SES.

> **Important**
>
> Consulte Configuración de las notificaciones de eventos para Amazon SES para obtener información importante sobre las notificaciones.

Temas

- Configuración de notificaciones de Amazon SNS para Amazon SES
- Contenidos de notificaciones de Amazon SNS para Amazon SES
- Ejemplos de notificaciones de Amazon SNS para Amazon SES

Configuración de notificaciones de Amazon SNS para Amazon SES

Amazon SES puede informarle de los rebotes, los reclamos y las entregas mediante Amazon Simple Notification Service (Amazon SNS).

Puede configurar las notificaciones en la consola de Amazon SES o mediante la API de Amazon SES.

Temas de esta sección:

- Requisitos previos
- Configuración de notificaciones con la consola de Amazon SES
- Configuración de notificaciones con la API de Amazon SES
- Solución de problemas de notificaciones de retroalimentación

Requisitos previos

Realice los pasos siguientes antes de configurar notificaciones de Amazon SNS en Amazon SES:

1. Cree un tema en Amazon SNS. Para obtener más información, consulte Creación de un tema en la Guía para desarrolladores de Amazon Simple Notification Service.

> **Important**
>
> Al crear un tema con Amazon SNS, en Type (Tipo), solo elija Standard (Estándar). (SES no admite temas de tipo FIFO).

Tanto si crea un nuevo tema de SNS como si selecciona uno existente, debe conceder acceso a SES para publicar notificaciones en el tema.

Para conceder permiso a Amazon SES para publicar notificaciones en el tema, en la pantalla Edit topic (Editar tema) de la consola de SNS, expanda Access policy (Política de acceso) y en el editor de JSON, agregue la siguiente política de permisos:

```
{
  "Version": "2012-10-17",
  "Id": "notification-policy",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ses.amazonaws.com"
      },
      "Action": "sns:Publish",
      "Resource": "arn:aws:sns:topic_region:111122223333:topic_name",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "111122223333",
          "AWS:SourceArn":
 "arn:aws:ses:topic_region:111122223333:identity/identity_name"
        }
      }
    }
  ]
}
```

En el ejemplo anterior de política, realice los siguientes cambios:

- Reemplace *topic_region* por la región de AWS en la que creó el tema de SNS.
- Reemplace *111122223333* por su ID de cuenta de AWS.

- Reemplace *topic_name* por el nombre del tema de SNS.
- Reemplace *identity_name* por la identidad verificada (dirección de correo electrónico o dominio) que se está suscribiendo al tema de SNS.

2. Suscriba al menos un punto de enlace al tema. Por ejemplo, si desea recibir notificaciones por mensaje de texto, suscriba un punto de enlace de SMS (es decir, un número de teléfono móvil) al tema. Para recibir notificaciones por correo electrónico, suscriba un punto de enlace de correo electrónico (una dirección de correo electrónico) al tema.

   Para obtener más información, consulte Introducción en la Guía para desarrolladores de Amazon Simple Notification Service.

3. (Opcional) Si su tema de Amazon SNS utiliza AWS Key Management Service (AWS KMS) para el cifrado del lado del servidor, tendrá que agregar permisos a la política de claves de AWS KMS. Puede añadir permisos asociando la siguiente política a la política de claves de AWS KMS:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSESToUseKMSKey",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

Configuración de notificaciones con la consola de Amazon SES

Para configurar notificaciones mediante la consola de Amazon SES

1. Abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.

2. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).
3. En el contenedor Identities (Identidades), seleccione la identidad verificada de la que desea recibir notificaciones de valoraciones cuando un mensaje enviado desde esta identidad produzca un rebote, un reclamo o una entrega.

> **Important**
>
> La configuración de notificaciones de dominio verificada se aplican a todos los correos electrónicos enviados desde las direcciones de correo electrónico en dicho dominio excepto para las direcciones de correo electrónico que también se han verificado.

4. En la pantalla de detalles de la identidad verificada que seleccionó, elija la pestaña Notifications (Notificaciones) y seleccione Edit (Editar) en el contenedor Feedback notifications (Notificaciones de valoración).
5. Expanda el cuadro de lista de temas de SNS de cada tipo de valoración para la que desee recibir notificaciones y seleccione un tema de SNS que le pertenezca, No SNS topic (Sin tema de SNS), o bien SNS topic you don't own (Tema de SNS que no le pertenece).

   - Si eligió SNS topic you don't own (Tema de SNS que no le pertenece), aparecerá el campo SNS topic ARN (ARN del tema de SNS) y deberá introducir el ARN del tema de SNS que el remitente delegado le ha compartido. (Solo el remitente delegado recibirá estas notificaciones porque es propietario del tema de SNS. Para obtener más información acerca de los envíos delegados, consulte Información general de la autorización de envío).

> **Important**
>
> Los temas de Amazon SNS que utiliza para las notificaciones de rebotes, reclamos y entregas deben estar en la misma Región de AWS en la que utiliza Amazon SES. Además, tiene que suscribir uno o varios puntos de enlace al tema para recibir notificaciones. Por ejemplo, si desea que las notificaciones se envíen a una dirección de correo electrónico, tiene que suscribir un punto de enlace de correo electrónico al tema. Para obtener más información, consulte Introducción en la Guía para desarrolladores de Amazon Simple Notification Service.

6. (Opcional) Si desea que la notificación del tema incluya los encabezados del correo electrónico original, marque la casilla Include original email headers (Incluir encabezados de correo

electrónico originales) directamente debajo del nombre del tema de SNS de cada tipo de valoración. Esta opción solo está disponible si ha asignado un tema de Amazon SNS al tipo de notificación asociado. Para obtener información sobre el contenido de los encabezados de correo electrónico originales, consulte el objeto `mail` en Contenido de las notificaciones.

7. Elija Save changes. Los cambios que haya realizado en su configuración de notificaciones podrían tardar varios minutos en surtir efecto.
8. (Opcional) Si eligió las notificaciones de tema de Amazon SNS tanto para rebotes como para reclamos, puede desactivar las notificaciones por correo electrónico en su totalidad para que no reciba notificaciones dobles a través de correo electrónico y notificaciones de SNS. Para desactivar las notificaciones por correo electrónico de rebotes y reclamos, en la pestaña Notifications (Notificaciones) en la pantalla de detalles de la identidad verificada, en el contenedor Email Feedback Forwarding (Reenvío de valoración de correo), elija Edit (Editar), desmarque la casilla Enabled (Habilitado), y elija Save changes (Guardar los cambios).

Después de configurar sus ajustes, comenzará a recibir notificaciones de rebotes, reclamos o entregas en sus temas de Amazon SNS. Estas notificaciones están en formato JavaScript Object Notation (JSON) y siguen la estructura que se describe en Contenido de las notificaciones.

Se le cobrarán las tarifas estándar de Amazon SNS para notificaciones de rebotes, reclamos y entregas. Para obtener más información, consulte la Página de precios de Amazon SNS.

> **Note**
>
> Si se produce un error al intentar publicar en el tema de Amazon SNS porque el tema se ha eliminado o la Cuenta de AWS ya no tiene permisos para publicar en él, Amazon SES eliminará la configuración de dicho tema si se ha configurado para rebotes o quejas (no para entregas; para las notificaciones de entrega, SES no eliminará la configuración de tema de SNS). Además, Amazon SES volverá a habilitar las notificaciones por correo electrónico de rebotes y reclamos para la identidad y se recibirá una notificación del cambio por correo electrónico. Si se configuran varias identidades para utilizar el tema, la configuración del tema de cada identidad cambia cuando cada identidad experimenta un error al publicar en el tema.

Configuración de notificaciones con la API de Amazon SES

También puede configurar notificaciones de rebotes, reclamos y entregas con la API de Amazon SES. Utilice las siguientes operaciones para configurar las notificaciones:

- SetIdentityNotificationTopic
- SetIdentityFeedbackForwardingEnabled
- GetIdentityNotificationAttributes
- SetIdentityHeadersInNotificationsEnabled

Puede utilizar estas acciones de la API para escribir una aplicación front-end personalizada para notificaciones. Para obtener una descripción completa de las acciones de la API relacionadas con las notificaciones, consulte la Referencia de la API de Amazon Simple Email Service.

Solución de problemas de notificaciones de retroalimentación

No recibir notificaciones

Si no recibe notificaciones, asegúrese de que ha suscrito un punto de enlace al tema a través del que se envían notificaciones. Cuando suscriba un punto de enlace de correo electrónico a un tema, recibirá un correo electrónico que le pedirá que confirme su suscripción. Debe confirmar su suscripción antes de empezar a recibir notificaciones por correo electrónico. Para obtener más información, consulte Introducción en la Guía para desarrolladores de Amazon Simple Notification Service.

Error **`InvalidParameterValue`** al elegir un tema

Si recibe un error que indica que se ha producido un error `InvalidParameterValue`, consulte el tema de Amazon SNS para ver si está cifrado con AWS KMS. Si es así, tendrá que modificar la política de la clave de AWS KMS. Consulte Requisitos previos para ver un ejemplo de política.

Contenidos de notificaciones de Amazon SNS para Amazon SES

Las notificaciones de rebotes, reclamos y entregas se publican en temas de Amazon Simple Notification Service (Amazon SNS) en formato JavaScript Object Notation (JSON). El objeto JSON de nivel superior contiene una cadena `notificationType`, un objeto `mail` y un objeto `bounce`, un objeto `complaint` o un objeto `delivery`.

Consulte las secciones siguientes para las descripciones de los diferentes tipos de objetos:

- Objeto JSON de nivel superior
- Objeto `mail`
- Objeto `bounce`
- Objeto `complaint`
- Objeto `delivery`

A continuación se muestran algunas notas importantes acerca del contenido de las notificaciones de Amazon SNS para Amazon SES:

- Para un tipo de notificación determinado, es posible que reciba una notificación de Amazon SNS para varios destinatarios o puede recibir una sola notificación de Amazon SNS por destinatario. El código debe ser capaz de analizar la notificación de Amazon SNS y gestionar ambos casos; Amazon SES no garantiza el orden ni la agrupación de las notificaciones enviadas a través de Amazon SNS. Sin embargo, distintos tipos de notificación de Amazon SNS (por ejemplo, rebotes y reclamos) nunca se combinan en una sola notificación.
- Podría recibir varios tipos de notificaciones de Amazon SNS para un destinatario. Por ejemplo, el servidor de correo electrónico receptor podría aceptar el correo electrónico (activando una notificación de entrega), pero después de procesar el correo electrónico, el servidor de correo electrónico receptor podría determinar que el correo electrónico da lugar en realidad a un rebote (desencadenando una notificación de rebote). Sin embargo, estas notificaciones siempre son independientes, ya que son tipos de notificación distintos.
- Amazon SES se reserva el derecho de agregar campos adicionales a las notificaciones. Por tanto, las aplicaciones que analizan estas notificaciones deben ser lo suficientemente flexibles como para gestionar campos desconocidos.
- Amazon SES sobrescribe los encabezados del mensaje cuando envía el correo electrónico. Puede recuperar los encabezados del mensaje original desde los campos `headers` y `commonHeaders` del objeto `mail`.

Objeto JSON de nivel superior

El objeto JSON de nivel superior de una notificación de Amazon SES contiene los siguientes campos.

Nombre del campo	Descripción
`notificationType`	Una cadena que contiene el tipo de notificación representado por el objeto JSON. Los valores posibles son `Bounce`, `Complaint` o `Delivery`. Si configuró la publicación de eventos, este campo se denomina `eventType`.
`mail`	Un objeto JSON que contiene información sobre el correo original al que pertenece la notificación. Para obtener más información, consulte Objeto Mail.
`bounce`	Este campo está presente solo si `notificationType` es `Bounce` y contiene un objeto JSON que mantiene información sobre el rebote. Para obtener más información, consulte Objeto Bounce.
`complaint`	Este campo está presente solo si `notificationType` es `Complaint` y contiene un objeto JSON que mantiene información sobre la reclamación. Para obtener más información, consulte Objeto Complaint.
`delivery`	Este campo está presente solo si `notificationType` es `Delivery` y contiene un objeto JSON que mantiene información sobre la entrega. Para obtener más información, consulte Objeto Delivery.

Objeto Mail

Cada notificación de rebote, reclamación o entrega contiene información sobre el correo electrónico original en el objeto `mail`. El objeto JSON que contiene información acerca de un objeto `mail` tiene los campos siguientes.

Nombre del campo	Descripción
`timestamp`	La hora a la que se ha enviado el mensaje original (en formato ISO8601).
`messageId`	Un ID exclusivo que Amazon SES asignó al mensaje. Amazon SES le devolvió este valor cuando envió el mensaje. **Note** Este ID de mensaje lo asignó Amazon SES. Puede encontrar el ID de mensaje del correo electrónico original en el campo `headers` del objeto `mail`.
`source`	La dirección de correo electrónico desde la que se envió el mensaje original (la dirección MAIL FROM del sobre).
`sourceArn`	El nombre de recurso de Amazon (ARN) de la identidad que se utilizó para enviar el correo electrónico. En el caso de una autorización de envío, el `sourceArn` es el ARN de la identidad que el propietario de la identidad autorizó utilizar al remitente delegado para enviar el correo electrónico. Para obtener más información acerca de la autorización de envío, consulte Métodos de autenticación del correo electrónico.

Nombre del campo	Descripción
`sourceIp`	La dirección IP pública de origen del cliente que realizó la solicitud de envío de correo electrónico a Amazon SES.
`sendingAccountId`	El ID de Cuenta de AWS de la cuenta que se utilizó para enviar el correo electrónico. En el caso de la autorización de envío, el `sendingAccountId` es el ID de cuenta del remitente delegado.
`callerIdentity`	La identidad de IAM del usuario de Amazon SES que ha enviado el correo electrónico.
`destination`	Una lista de direcciones de correo electrónico que han sido destinatarios del correo electrónico original.
`headersTruncated`	Este objeto solo está presente si configuró la configuración de las notificaciones para incluir los encabezados del correo electrónico original. Indica si los encabezados están truncados en la notificación. Amazon SES trunca los encabezados en la notificación cuando los encabezados del mensaje original tienen un tamaño de 10 KB o superior. Los posibles valores son `true` y `false`.

Nombre del campo	Descripción
`headers`	Este objeto solo está presente si configuró la configuración de las notificaciones para incluir los encabezados del correo electrónico original. Una lista de los encabezados originales del correo electrónico. Cada encabezado de la lista tiene un campo `name` y un campo `value`. **Note** Cualquier ID de mensaje dentro del objeto `headers` procede del mensaje original que pasó a Amazon SES. El ID de mensaje que Amazon SES asignó seguidamente al mensaje está en el campo `messageId` del objeto `mail`.

Nombre del campo	Descripción
`commonHeaders`	Este objeto solo está presente si configuró la configuración de las notificaciones para incluir los encabezados del correo electrónico original. Incluye información sobre los encabezados de correo electrónico comunes del correo electrónico original, incluido los campos Desde, A y Asunto. Dentro de este objeto, cada encabezado es una clave. Los campos Desde y A se representan por matrices que contienen varios valores. **Note** Para eventos, el ID de mensaje dentro del campo `commonHeaders` es el ID de mensaje que Amazon SES asignó seguidamente al mensaje en el campo `messageId` del objeto del correo. Las notificaciones contendrán el ID de mensaje del correo electrónico original.

A continuación, se muestra un ejemplo de un objeto `mail` que incluye los encabezados de correo electrónico originales. Cuando este tipo de notificación no está configurado para incluir los encabezados de correo electrónico originales, el objeto `mail` no incluye los campos `headersTruncated`, `headers` y `commonHeaders`.

```
{
   "timestamp":"2018-10-08T14:05:45 +0000",
   "messageId":"000001378603177f-7a5433e7-8edb-42ae-af10-f0181f34d6ee-000000",
   "source":"sender@example.com",
   "sourceArn": "arn:aws:ses:us-east-1:888888888888:identity/example.com",
   "sourceIp": "127.0.3.0",
   "sendingAccountId":"123456789012",
   "destination":[
```

```
      "recipient@example.com"
   ],
   "headersTruncated":false,
   "headers":[
      {
         "name":"From",
         "value":"\"Sender Name\" <sender@example.com>"
      },
      {
         "name":"To",
         "value":"\"Recipient Name\" <recipient@example.com>"
      },
      {
         "name":"Message-ID",
         "value":"custom-message-ID"
      },
      {
         "name":"Subject",
         "value":"Hello"
      },
      {
         "name":"Content-Type",
         "value":"text/plain; charset=\"UTF-8\""
      },
      {
         "name":"Content-Transfer-Encoding",
         "value":"base64"
      },
      {
         "name":"Date",
         "value":"Mon, 08 Oct 2018 14:05:45 +0000"
      }
   ],
   "commonHeaders":{
      "from":[
         "Sender Name <sender@example.com>"
      ],
      "date":"Mon, 08 Oct 2018 14:05:45 +0000",
      "to":[
         "Recipient Name <recipient@example.com>"
      ],
      "messageId":" custom-message-ID",
      "subject":"Message sent using Amazon SES"
   }
```

```
}
```

Objeto Bounce

El objeto JSON que contiene información acerca de rebotes contiene los campos siguientes.

Nombre del campo	Descripción
`bounceType`	El tipo de rebote, tal como determina Amazon SES. Para obtener más información, consulte Tipos de rebote.
`bounceSubType`	El subtipo de rebote, tal como determina Amazon SES. Para obtener más información, consulte Tipos de rebote.
`bouncedRecipients`	Una lista que contiene información acerca de los destinatarios del mensaje de correo electrónico original que dio lugar a un rebote. Para obtener más información, consulte Destinatarios con rebote.
`timestamp`	La fecha y la hora a la que se ha enviado el rebote (en formato ISO8601). Tenga en cuenta que se trata de la hora a la que el ISP envió la notificación y no la hora a la que la recibió Amazon SES.
`feedbackId`	Un ID único para el rebote.

Si Amazon SES pudo contactar con la autoridad de transferencia de mensajes (MTA) remota, también está presente el siguiente campo.

Nombre del campo	Descripción
`remoteMtaIp`	La dirección IP de la MTA a la que Amazon SES intentó entregar el correo electrónico.

Si se adjunta una notificación de estado de entrega (DSN) al rebote, también está presente el siguiente campo.

Nombre del campo	Descripción
`reportingMTA`	El valor del campo `Reporting-MTA` del DSN. Se trata del valor de la autoridad de transferencia de mensajes (MTA) que intentó realizar la operación de entrega, retransmisión o gateway descrita en el DSN.

A continuación se muestra un ejemplo de un objeto `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"
}
```

Destinatarios con rebote

Una notificación de rebote podría pertenecer a un único destinatario o a varios destinatarios. El campo `bouncedRecipients` aloja una lista de objetos (un objeto por destinatario a quien pertenece la notificación de rebote) y siempre contiene el campo siguiente.

Nombre del campo	Descripción
`emailAddress`	La dirección de correo electrónico del destinatario. Si hay un DSN disponible, se trata del valor del campo `Final-Recipient` del DSN.

Opcionalmente, si hay un DSN adjunto al rebote, los siguientes campos también podrían estar presentes.

Nombre del campo	Descripción
`action`	El valor del campo `Action` del DSN. Esto indica la acción que realiza el Reporting-MTA como resultado de su intento de entregar el mensaje a este destinatario.
`status`	El valor del campo `Status` del DSN. Se trata del código de estado independiente del transporte por destinatario que indica el estado de entrega del mensaje.
`diagnosticCode`	El código de estado emitido por la MTA de notificación. Este es el valor del campo `Diagnostic-Code` del DSN. Este campo puede estar ausente en el DSN (y, por lo tanto, también ausente en el JSON).

A continuación se muestra un ejemplo de objeto que podría estar en la lista `bouncedRecipients`.

```
{
    "emailAddress": "recipient@example.com",
    "action": "failed",
    "status": "5.0.0",
    "diagnosticCode": "X-Postfix; unknown user"
}
```

Tipos de rebote

El objeto de rebote contiene un tipo de rebote `Undetermined`, `Permanent` o `Transient`. Los tipos de rebote `Permanent` y `Transient` también pueden contener uno de varios subtipos de rebote.

Cuando reciba una notificación de rebote con un tipo `Transient`, es posible que pueda enviar correo electrónico a ese destinatario en el futuro si se resuelve el problema que provocó el rebote del mensaje.

Cuando recibes una notificación de rebote con un tipo `Permanent`, es poco probable que pueda enviar correo electrónico a ese destinatario en el futuro. Por este motivo, debe quitar inmediatamente el destinatario cuya dirección produjo el rebote de las listas de correo.

> **Note**
>
> Cuando se produce un rebote temporal (un rebote relacionado con un problema temporal, por ejemplo, que se llene la bandeja de correo del destinatario), Amazon SES intenta entregar de nuevo el correo electrónico durante un determinado periodo de tiempo. Al final de ese periodo de tiempo, si Amazon SES sigue sin poder entregar el correo electrónico, deja de intentarlo.
> Amazon SES ofrece notificaciones de los rebotes permanentes, así como de los rebotes temporales cuya entrega ha dejado de intentar. Si desea recibir una notificación cada vez que se produzca un rebote temporal, habilite la publicación de eventos y configúrela para que envíe notificaciones cuando se produzcan eventos en de retraso en la entrega.

bounceType	bounceSubType	Descripción
`Undetermined`	`Undetermined`	El proveedor de correo electrónico del destinatario envió un mensaje de rebote. El mensaje de rebote no contenía información suficiente para que Amazon SES determinara el motivo del rebote. El correo electrónico de rebote, que se envió a la dirección del encabezado Return-Path del correo electrónico que generó el rebote, podría contener información adicional sobre el problema que provocó que rebotara el correo electrónico.

bounceType	bounceSubType	Descripción
`Permanent`	`General`	El proveedor de correo electrónico del destinatario envió un mensaje de devolución permanente. **Important** Cuando reciba este tipo de notificación de rebote, debe quitar inmediatamente la dirección de correo electrónico del destinatario de su lista de correo. El envío de mensajes a direcciones que producen rebotes permanentes puede tener un impacto negativo en su reputación como remitente. Si sigue enviando correos electrónicos a direcciones que producen rebotes permanentes, podríamos detener su capacidad para enviar correo electrónico adicional. Consulte the section called “Uso de la lista de supresión de nivel de cuenta”.
`Permanent`	`NoEmail`	No fue posible recuperar la dirección de correo electrónico del destinatario del mensaje de rebote.
`Permanent`	`Suppressed`	La dirección de correo electrónico del destinatario está en la lista de supresión de Amazon SES porque tiene un historial reciente de generar rebotes permanentes. Para anular la lista de supresión global, consulte Uso de la lista de supresión de nivel de cuenta de Amazon SES.

bounceType	bounceSubType	Descripción
`Permanent`	`OnAccountSuppressionList`	Amazon SES ha suprimido el envío a esta dirección porque está en la lista de supresión de nivel de cuenta. Esto no se toma en cuenta para calcular la métrica de porcentaje de rebotes.
`Transient`	`General`	El proveedor de correo electrónico del destinatario envió un mensaje de rebote general. Puede enviar un mensaje al mismo destinatario en el futuro si se resolviera el problema que provocó el rebote del mensaje. **Note** Si envía un correo electrónico a un destinatario que tiene una regla de respuesta automática activa (como, por ejemplo, un mensaje de "fuera de la oficina"), es posible que reciba este tipo de notificación. Aunque la respuesta tiene un tipo de notificación `Bounce`, Amazon SES no cuenta las respuestas automáticas cuando calcula la tasa de rebotes de su cuenta.
`Transient`	`MailboxFull`	El proveedor de correo electrónico del destinatario envió un mensaje de rebote porque la bandeja de entrada del destinatario estaba llena. Podría realizar el envío al mismo destinatario en el futuro cuando la bandeja de entrada deje de estar llena.

bounceType	bounceSubType	Descripción
`Transient`	`MessageTooLarge`	El proveedor de correo electrónico del destinatario envió un mensaje de rebote porque el mensaje enviado era demasiado grande. Podría enviar un mensaje al mismo destinatario si reduce el tamaño del mensaje.
`Transient`	`ContentRejected`	El proveedor de correo electrónico del destinatario envió un mensaje de rebote porque el mensaje enviado incluye contenido que el proveedor no permite. Podría enviar un mensaje al mismo destinatario si cambia el contenido del mensaje.
`Transient`	`AttachmentRejected`	El proveedor de correo electrónico del destinatario envió un mensaje de rebote porque el mensaje contenía un archivo adjunto inaceptable. Por ejemplo, algunos proveedores de correo electrónico pueden rechazar mensajes con archivos adjuntos de un determinado tipo de archivo o mensajes con archivos adjuntos muy grandes. Podría enviar un mensaje al mismo destinatario si quita o cambia el contenido del archivo adjunto.

Objeto Complaint

El objeto JSON que contiene información acerca de reclamaciones tiene los campos siguientes.

Nombre del campo	Descripción
`complainedRecipients`	Una lista que contiene información sobre destinatarios que podrían haber sido responsables de la reclamación. Para obtener más información, consulte Destinatarios con reclamaciones.

Nombre del campo	Descripción
`timestamp`	La fecha y la hora a la que el ISP envió la notificación de reclamación, en formato ISO 8601. La fecha y la hora de este campo podrían no ser las mismas en que Amazon SES recibió la notificación.
`feedbackId`	Un ID único asociado con la reclamación.
`complaintSubType`	El valor del campo `complaintSubType` puede ser nulo o `OnAccountSuppressionList` . Si el valor es `OnAccountSuppressionList` , Amazon SES aceptó el mensaje, pero no intentó enviarlo porque estaba en la lista de supresión de nivel de cuenta.

Además, si se adjunta un informe de retroalimentación a la reclamación, podrían estar presentes los siguientes campos.

Nombre del campo	Descripción
`userAgent`	El valor del campo `User-Agent` del informe de retroalimentación. Esto indica el nombre y la versión del sistema que generó el informe.
`complaintFeedbackType`	El valor del campo `Feedback-Type` del informe de retroalimentación recibido desde el ISP. Contiene el tipo de retroalimentación.
`arrivalDate`	El valor del campo `Arrival-Date` o `Received-Date` del informe de retroalimentación (en formato ISO8601). Este campo puede estar ausente en el informe (y, por lo tanto, también ausente en el JSON).

A continuación se muestra un ejemplo de un objeto `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"
}
```

Destinatarios con reclamaciones

El campo `complainedRecipients` contiene una lista de destinatarios que podrían haber enviado la reclamación. Debe utilizar esta información para determinar qué destinatario envió la reclamación y, a continuación, quitar inmediatamente a ese destinatario de sus listas de correo.

> **Important**
>
> La mayoría de los ISP eliminan la dirección de correo electrónico del destinatario que envió la reclamación de su notificación de reclamación. Por este motivo, esta lista contiene información acerca de los destinatarios que podrían haber enviado el reclamo, en función de los destinatarios del mensaje original y el ISP del que hemos recibido el reclamo. Amazon SES realiza una búsqueda en el mensaje original para determinar esta lista de destinatarios.

Los objetos JSON de esta lista contienen el siguiente campo.

Nombre del campo	Descripción
`emailAddress`	La dirección de correo electrónico del destinatario.

A continuación se muestra un ejemplo de un objeto de destinatario con reclamo.

```
{ "emailAddress": "recipient1@example.com" }
```

> **Note**
>
> Debido a este comportamiento, puede estar más seguro de que sabe qué dirección de correo electrónico ha presentado una reclamación por su mensaje si limita el envío a un mensaje por destinatario (en lugar de enviar un mensaje con 30 direcciones de correo electrónico distintas en la línea CCO).

Tipos de reclamación

Es posible que vea los siguientes tipos de reclamación en el campo `complaintFeedbackType` tal como los ha asignado el ISP que realiza la notificación, de acuerdo con el sitio web de Internet Assigned Numbers Authority:

- `abuse`: indica correo electrónico no solicitado o algún otro tipo de abuso de correo electrónico.
- `auth-failure`: informe de error de autenticación de correo electrónico.
- `fraud`: indica algún tipo de fraude o actividad de phishing.
- `not-spam`: indica que la entidad que proporciona el informe no considera el mensaje como spam. Esto se puede utilizar para corregir un mensaje que estaba mal etiquetado o clasificado como spam.
- `other`: indica cualquier otra retroalimentación que no encaje en otros tipos registrados.
- `virus`: notifica que se ha encontrado un virus en el mensaje de origen.

Objeto Delivery

El objeto JSON que contiene información sobre entregas tiene siempre los campos siguientes.

Nombre del campo	Descripción
`timestamp`	La hora a la que Amazon SES entregó el correo electrónico al servidor de correo del destinatario (en formato ISO8601).
`processingTimeMillis`	El tiempo en milisegundos desde el momento en que Amazon SES; acepta la solicitud del

Nombre del campo	Descripción
	remitente para transferir el mensaje al servidor de correo del destinatario.
`recipients`	Una lista de sus destinatarios de los correos electrónicos a los que corresponde la notificac ión de entrega.
`smtpResponse`	El mensaje de respuesta SMTP del ISP remoto que ha aceptado el correo electrónico desde Amazon SES. Este mensaje varía por correo electrónico, por servidor de correo electrónico de recepción y por ISP de recepción.
`reportingMTA`	El nombre de host del servidor de correo electrónico de Amazon SES que envió el correo electrónico.
`remoteMtaIp`	La dirección IP de la MTA a la que Amazon SES entregó el correo electrónico.

A continuación se muestra un ejemplo de un objeto `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"
}
```

Ejemplos de notificaciones de Amazon SNS para Amazon SES

En las secciones siguientes se ofrecen ejemplos de los tres tipos de notificaciones:

- Para obtener ejemplos de notificaciones de rebote, consulte Ejemplos de notificaciones de rebote de Amazon SNS.

- Para obtener ejemplos de notificaciones de reclamaciones, consulte Ejemplos de notificaciones de reclamos de Amazon SNS.
- Para obtener ejemplos de notificaciones de entrega, consulte Ejemplo de notificación de entrega de Amazon SNS.

Ejemplos de notificaciones de rebote de Amazon SNS

Esta sección contiene ejemplos de notificaciones de rebote con y sin una notificación de estado de entrega (DSN) proporcionada por el receptor de correo electrónico que envió la retroalimentación.

Notificación de rebote con una DSN

A continuación, se muestra un ejemplo de una notificación de rebote que contiene una DSN y los encabezados de correo electrónico originales. Cuando las notificaciones de rebote no se configuran para incluir los encabezados de correo electrónico originales, el objeto `mail` con las notificaciones no incluye los campos `headersTruncated`, `headers` y `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"
          }
       }
   }
```

Notificación de rebote sin DSN

A continuación, se muestra un ejemplo de una notificación de rebote que incluye los encabezados de correo electrónico originales pero no incluye una DSN. Cuando las notificaciones de rebote no se configuran para incluir los encabezados de correo electrónico originales, el objeto `mail` con las notificaciones no incluye los campos `headersTruncated`, `headers` y `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"
       }
    }
}
```

Ejemplos de notificaciones de reclamos de Amazon SNS

Esta sección contiene ejemplos de notificaciones de reclamos con y sin un informe de retroalimentación proporcionado por el receptor de correo electrónico que envió el comentario.

Notificación de reclamo con un informe de retroalimentación

A continuación, se muestra un ejemplo de una notificación de reclamación que contiene un informe de retroalimentación y los encabezados de correo electrónico originales. Cuando las notificaciones de reclamación no se configuran para incluir los encabezados de correo electrónico originales, el objeto `mail` con las notificaciones no incluye los campos `headersTruncated`, `headers` y `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"
       }
    }
}
```

Notificación de reclamo sin informe de retroalimentación

A continuación, se muestra un ejemplo de una notificación de reclamación que incluye los encabezados de correo electrónico originales, pero no incluye un informe de retroalimentación. Cuando las notificaciones de reclamación no se configuran para incluir los encabezados de correo electrónico originales, el objeto `mail` con las notificaciones no incluye los campos `headersTruncated`, `headers` y `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"
          }
       }
  }
```

Ejemplo de notificación de entrega de Amazon SNS

A continuación, se muestra un ejemplo de una notificación de entrega que incluye los encabezados de correo electrónico originales. Cuando las notificaciones de entrega no se configuran para incluir los encabezados de correo electrónico originales, el objeto `mail` con las notificaciones no incluye los campos `headersTruncated`, `headers` y `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"
    }
}
```

Uso de la autorización de identidad en Amazon SES

Las políticas de autorización de identidad definen cómo las identidades verificadas individuales pueden utilizar Amazon SES especificando qué acciones de la API de SES están permitidas o rechazadas para la identidad y en qué condiciones.

Con el uso de estas políticas de autorización, podrá mantener el control sobre sus identidades cambiando o revocando los permisos en cualquier momento. Incluso puede autorizar que otros usuarios usen las identidades de su propiedad (dominios o direcciones de correo electrónico) mediante sus propias cuentas de SES.

Temas

- Anatomía de las políticas de Amazon SES
- Creación de una política de autorización de identidad en Amazon SES
- Ejemplos de políticas de identidad en Amazon SES
- Administración de las políticas de autorización de identidad de Amazon SES

Anatomía de las políticas de Amazon SES

Las directivas se adhieren a una estructura específica, contienen elementos y deben cumplir ciertos requisitos.

Estructura de la política

Cada política de autorización es un documento JSON asociado a una identidad. Cada política incluye las siguientes secciones.

- Información aplicable a toda la política en la parte superior del documento.
- Una o varias instrucciones individuales, cada una de las cuales describe un conjunto de permisos.

La siguiente política de ejemplo otorga al ID de cuenta de AWS 123456789012 los permisos especificados en la sección Acción para el dominio verificado example.com.

```
{
  "Id":"ExampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeAccount",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:123456789012:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
      "Action":[
        "ses:GetEmailIdentity",
        "ses:UpdateEmailIdentityPolicy",
        "ses:ListRecommendations",
        "ses:CreateEmailIdentityPolicy",
```

```
        "ses:DeleteEmailIdentity"
      ]
    }
  ]
}
```

Encontrará más ejemplos de política de autorización en Ejemplos de políticas de identidad.

Elementos de una política

Esta sección describe los elementos que contienen las políticas de autorización de identidad. En primer lugar, describimos elementos aplicables a toda la política y, a continuación, describimos los elementos que se aplican únicamente a la instrucción en la que están incluidos. Se sigue con una exposición sobre cómo añadir condiciones a sus instrucciones.

Para obtener información específica acerca de la sintaxis de los elementos, consulte Gramática del lenguaje de las políticas de IAM en la Guía del usuario de IAM.

Información aplicable a toda la política

Existen dos elementos a escala de política: `Id` y `Version`. La tabla siguiente proporciona información acerca de estos elementos.

Nombre	Descripción	Obligatorio	Valores válidos
`Id`	Identifica de forma exclusiva la política.	No	Cualquier cadena
`Version`	Especifica la versión de idioma de acceso de la política.	No	Cualquier cadena. Como práctica recomendada, le aconsejamos que incluya este campo con un valor de "2012-10-17".

Instrucciones específicas de la política

Las políticas de autorización de identidad requieren al menos una instrucción. Cada instrucción puede incluir los elementos que se describen en la siguiente tabla.

Nombre	Descripción	Obligatorio	Valores válidos
`Sid`	Identifica de forma exclusiva la instrucción.	No	Cualquier cadena.
`Effect`	Especifica el resultado que desea que devuelva la instrucción de política en tiempo de evaluación.	Sí	"Allow" o "Deny".
`Resource`	Especifica la identidad a la que se aplica la política. (Esta es la dirección de correo electrónico o dominio que el propietario de identidad autoriza utilizar al remitente delegado para autorización de envío).	Sí	El nombre de recurso de Amazon (ARN) de la identidad.
`Principal`	Especifica la Cuenta de AWS, el usuario o el servicio de AWS que recibe el permiso en la instrucción.	Sí	ID de Cuenta de AWS válido, ARN de usuario o servicio de AWS. Cuenta de AWS Los ID y ARN de usuario se especifican mediante `"AWS"` (por ejemplo, `"AWS": ["123456789012"]` o

Nombre	Descripción	Obligatorio	Valores válidos
			`"AWS": ["arn:aws:iam::123456789012:root"]`). Los nombres de servicios de AWS se especifican mediante `"Service"` (por ejemplo, `"Service": ["cognito-idp.amazonaws.com"]`). Para ver ejemplos del formato de los ARN de usuario, consulte la Referencia general de AWS.

Nombre	Descripción	Obligatorio	Valores válidos
`Action`	Especifica la acción a la que se refiere la instrucción.	Sí	"ses:BatchGetMetricData", "ses:CancelExportJob", "ses:CreateDeliverabilityTestReport", "ses:CreateEmailIdentityPolicy", "ses:CreateExportJob", "ses:DeleteEmailIdentity", "ses:DeleteEmailIdentityPolicy", "ses:GetDomainStatisticsReport", "ses:GetEmailIdentity","ses:GetEmailIdentityPolicies", "ses:GetExportJob", "ses:ListExportJobs", "ses:ListRecommendations", "ses:PutEmailIdentityConfigurationSetAttributes", "ses:PutEmailIdentityDkimAttributes", "ses:PutEmailIdentityDkimSigningAttributes", "ses:PutEmailIdentityFeedbackAttributes", "ses:PutEmailIdentityMailFromAttributes", "ses:TagResource",

Nombre	Descripción	Obligatorio	Valores válidos
			"ses:UntagResource", "ses:UpdateEmailIdentityPolicy" (Acciones Autorización de envío: "ses:SendEmail", "ses:SendRawEmail", "ses:SendTemplatedEmail", "ses:SendBulkTemplatedEmail") Puede especificar una o varias de estas operaciones.
`Condition`	Especifica alguna limitación o información sobre el permiso.	No	Consulte la información acerca de las condiciones siguiendo esta tabla.

Condiciones

Una condición es cualquier restricción sobre el permiso en la instrucción. La parte de la instrucción que especifica las condiciones puede ser la más detallada de todas las partes. Una clave es la característica específica que es la base para la restricción de acceso, como la fecha y hora de la solicitud.

Las condiciones y las claves se utilizan conjuntamente para expresar la restricción. Por ejemplo, si desea impedir que el remitente delegado realice solicitudes a Amazon SES en su nombre después del 30 de julio de 2019, utilice la condición denominada `DateLessThan`. Usted utiliza la clave denominada `aws:CurrentTime` y la define con el valor `2019-07-30T00:00:00Z`.

SES implementa solo las claves de políticas a escala de AWS que se indican a continuación:

- `aws:CurrentTime`
- `aws:EpochTime`

- `aws:SecureTransport`
- `aws:SourceIp`
- `aws:SourceVpc`
- `aws:SourceVpce`
- `aws:UserAgent`
- `aws:VpcSourceIp`

Para obtener más información acerca de estas claves, consulte la Guía del usuario de IAM.

Requisitos de política

Las políticas deben cumplir todos los requisitos siguientes:

- Cada política tiene que incluir al menos una instrucción.
- Cada política tiene que incluir al menos una entidad principal válida.
- Cada política tiene que especificar un recurso y ese recurso debe ser el ARN de la identidad a la que está asociada la política.
- Los propietarios de identidad pueden asociar hasta 20 políticas con cada identidad única.
- Las políticas no pueden tener más de 4 kilobytes (KB) de tamaño.
- Los nombres de política no pueden superar los 64 caracteres. Además, solo pueden incluir caracteres alfanuméricos, guiones y guiones bajos.

Creación de una política de autorización de identidad en Amazon SES

Una política de autorización de identidad se compone de instrucciones que especifican qué acciones de la API están permitidas o denegadas para una identidad y en qué condiciones.

Para autorizar a un dominio de Amazon SES o a una identidad de dirección de correo electrónico de su propiedad, debe crear una política de autorización y, a continuación, adjuntar dicha política a la identidad. Una identidad puede tener cero, una o varias políticas. Sin embargo, una única política solo se puede asociar a una única identidad.

Para obtener una lista de las acciones de la API que se pueden usar en una política de autorización de envío, consulte la fila Acción de la tabla the section called “Instrucciones específicas de la política”.

Puede crear una política de autorización de envío de las siguientes formas:

- Mediante el generador de políticas: puede crear una política sencilla utilizando el generador de políticas de la consola de SES. Además de permitir o denegar permisos en las acciones de la API de SES, puede restringir las acciones con condiciones. También puede usar el generador de políticas para crear la estructura básica de una política y, a continuación, personalizarla más adelante editando la política.
- Mediante la creación de una política personalizada: si desea incluir condiciones más avanzadas o utilizar un servicio de AWS como entidad principal, puede crear una política personalizada y adjuntarla a la identidad a través de la consola de SES o la API de SES.

Temas

- Uso del generador de políticas
- Creación de una política personalizada

Uso del generador de políticas

Puede usar el generador de políticas para crear una política de autorización sencilla mediante los pasos que se indican a continuación.

Para crear una política mediante el generador de políticas

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).
3. En el contenedor Identities (Identidades) en la pantalla Verified identities (Identidades verificadas), seleccione la identidad verificada para la que desea crear una política de autorización.
4. En la pantalla de detalles de la identidad verificada que seleccionó en el paso anterior, elija la pestaña Authorization (Autorización).
5. En el panel Authorization policies (Políticas de autorización), elija Create policy (Crear política) y seleccione Use policy generator (Utilizar generador de políticas) en el menú desplegable.
6. En el panel Create statement (Crear instrucción), elija Allow (Permitir) en el campo Effect (Efecto). (Si desea crear una política para restringir esta identidad, elija Deny (Rechazar) en su lugar).

7. En el campo Principals (Entidades principales), indique el Cuenta de AWS ID, el ARN del usuario de IAM o el servicio AWS para recibir los permisos que quiere autorizar para esta identidad y, a continuación, elija Add (Añadir). (Si desea autorizar a más de una, repita este paso para cada una).
8. En el campo Actions (Acciones), marque la casilla de verificación de cada acción que desea autorizar para sus entidades principales.
9. (Opcional) Expanda Specify conditions (Especificar condiciones) si desea añadir una instrucción calificada al permiso.

    a. Seleccione un operador de la lista desplegable Operator (Operador).
    b. Seleccione un tipo de la lista desplegable Key (Clave).
    c. Respecto del tipo de clave que ha seleccionado, introduzca su valor en el campo Value (Valor). (Si desea agregar más condiciones, elija Add new condition [Agregar nueva condición] y repita este paso para cada condición adicional.)
10. Elija Save statement (Guardar instrucción).
11. (Opcional) Expanda Create another statement (Crear otra instrucción) si desea agregar más instrucciones a su política y repita los pasos 6 a 10.
12. Elija Next (Siguiente) y, en la pantalla Customize policy (Personalizar política), el contenedor Edit policy details (Editar detalles de la política) incluye campos en los que puede cambiar o personalizar el Name (Nombre) y el Policy document (Documento de la política).
13. Elija Next (Siguiente) y en la pantalla Review and apply (Revisar y aplicar), el contenedor Overview (Información general) mostrará la identidad verificada que está autorizando, así como el nombre de esta política. En el panel Policy document (Documento de la política) encontrará la política real que acaba de escribir junto con cualquier condición que haya agregado: revise la política y, si parece correcta, elija Apply policy (Aplicar política). (Si necesita cambiar o corregir algo, elija Previous [Anterior] y trabaje en el contenedor Edit policy details [Editar detalles de la política].

Creación de una política personalizada

Si desea crear una política personalizada y asociarla a una identidad, dispone de las siguientes opciones:

- Mediante la API de Amazon SES: cree una política en un editor de texto y, a continuación, adjúntela a la identidad a través de la API de `PutIdentityPolicy`, que se describe en la Referencia de la API de Amazon Simple Email Service.

- Mediante la consola de Amazon SES: cree una política en un editor de texto y adjúntela a una identidad pegándola en el editor de políticas personalizadas en la consola de Amazon SES. El siguiente procedimiento describe este método.

Para crear una política personalizada utilizando el editor de políticas personalizadas

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).
3. En el contenedor Identities (Identidades) en la pantalla Verified identities (Identidades verificadas), seleccione la identidad verificada para la que desea crear una política de autorización.
4. En la pantalla de detalles de la identidad verificada que seleccionó en el paso anterior, elija la pestaña Authorization (Autorización).
5. En el panel Authorization policies (Políticas de autorización), elija Create policy (Crear política) y seleccione Create custom policy (Crear política personalizada) en el menú desplegable.
6. En el panel Policy document (Documento de la política), pegue el texto de su política en formato JSON. También puede usar el generador de políticas para crear rápidamente la estructura básica de una política y, a continuación, personalizarla aquí.
7. Seleccione Apply Policy. (Si alguna vez necesita modificar su política personalizada, marque la casilla de verificación debajo de la pestaña Authorization [Autorización], elija Edit [Editar] y realice los cambios en el panel Policy document (Documento de la política), seguido de Save changes [Guardar los cambios]).

Ejemplos de políticas de identidad en Amazon SES

La autorización de identidad le permite especificar las condiciones detalladas en las que permite o deniega las acciones de la API para una identidad.

Los siguientes ejemplos muestran cómo escribir políticas para controlar distintos aspectos de las acciones de la API:

- Especificación de la entidad principal
- Restricción de la acción

- Uso de varias instrucciones

Especificación de la entidad principal

La entidad principal, que es la entidad a la que se conceden los permisos, puede ser una Cuenta de AWS, un usuario de AWS Identity and Access Management (IAM) o un servicio de AWS que pertenece a la misma cuenta.

El siguiente ejemplo muestra una política sencilla que permite al ID de AWS 123456789012 controlar la identidad verificada example.com (que también es propiedad de Cuenta de AWS 123456789012).

```
{
  "Id":"SampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeMarketer",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:123456789012:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
      "Action":[
        "ses:DeleteEmailIdentity",
        "ses:PutEmailIdentityDkimSigningAttributes"
      ]
    }
  ]
}
```

La siguiente política de ejemplo otorga permiso a dos usuarios para controlar la identidad verificada example.com. Los usuarios se especifican por su nombre de recurso de Amazon (ARN).

```
{
  "Id":"ExampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeIAMUser",
      "Effect":"Allow",
```

```
      "Resource":"arn:aws:ses:us-east-1:123456789012:identity/example.com",
      "Principal":{
        "AWS":[
          "arn:aws:iam::123456789012:user/John",
          "arn:aws:iam::123456789012:user/Jane"
        ]
      },
      "Action":[
        "ses:DeleteEmailIdentity",
        "ses:PutEmailIdentityDkimSigningAttributes"
      ]
    }
  ]
}
```

Restricción de la acción

Se pueden especificar varias acciones en una política de autorización de identidad en función del nivel de control que desee autorizar:

```
"BatchGetMetricData",
"ListRecommendations",
"CreateDeliverabilityTestReport",
"CreateEmailIdentityPolicy",
"DeleteEmailIdentity",
"DeleteEmailIdentityPolicy",
"GetDomainStatisticsReport",
"GetEmailIdentity",
"GetEmailIdentityPolicies",
"PutEmailIdentityConfigurationSetAttributes",
"PutEmailIdentityDkimAttributes",
"PutEmailIdentityDkimSigningAttributes",
"PutEmailIdentityFeedbackAttributes",
"PutEmailIdentityMailFromAttributes",
"TagResource",
"UntagResource",
"UpdateEmailIdentityPolicy"
```

Las políticas de autorización de identidad también le permiten restringir la entidad principal a solo una de esas acciones.

```
{
  "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
      ]
    }
  ]
}
```

Uso de varias instrucciones

Su política de autorización de envío puede incluir varias instrucciones. La siguiente política de ejemplo contiene dos instrucciones. La primera instrucción niega a dos usuarios el acceso a `getemailidentity` de sender@example.com desde de la misma cuenta `123456789012`. La segunda instrucción niega `UpdateEmailIdentityPolicy` a la entidad principal, Jack, dentro de la misma cuenta `123456789012`.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"DenyGet",
      "Effect":"Deny",
      "Resource":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
      "Principal":{
        "AWS":[
          "arn:aws:iam::123456789012:user/John",
          "arn:aws:iam::123456789012:user/Jane"
        ]
      },
      "Action":[
        "ses:GetEmailIdentity"
      ]
    },
```

```
    {
      "Sid":"DenyUpdate",
      "Effect":"Deny",
      "Resource":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
      "Principal":{
        "AWS":"arn:aws:iam::123456789012:user/Jack"
      },
      "Action":[
        "ses:UpdateEmailIdentityPolicy"
      ]
    }
  ]
}
```

Administración de las políticas de autorización de identidad de Amazon SES

Además de crear y asociar políticas a identidades, puede editar, quitar, enumerar y recuperar las políticas de una identidad, tal y como se describe en las secciones siguientes.

Administración de políticas mediante la consola de Amazon SES

La administración de las políticas de Amazon SES permite visualizar, editar o eliminar una política asociada a una identidad mediante la consola de Amazon SES.

Para administrar políticas en Amazon SES mediante la consola

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, elija Verified identities (Identidades verificadas).
3. En la lista de identidades, elija la identidad que desea administrar.
4. En la página de detalles de la identidad, diríjase a la pestaña Authorization (Autorización). Aquí encontrará una lista de todas las políticas adjuntas a esta identidad.
5. Seleccione la política que desea administrar al marcar la casilla de verificación correspondiente.
6. En función de la tarea de administración deseada, elija el botón correspondiente de la siguiente manera:

    a. Para visualizar una política, elija View policy (Visualizar política). Si necesita copiarla, elija el botón Copy (Copiar) y se copiará en su portapapeles.
    b. Para editar la política, elija Edit (Editar). En el panel Policy document (Documento de la política), edite la política, y luego elija Save changes (Guardar los cambios).

> **Note**
>
> Para revocar los permisos, puede editar la política o eliminarla.

c. Para eliminar la política, elija Delete (Borrar).

> **Important**
>
> Eliminar una política es una acción permanente. Le recomendamos que copie y pegue la política en un archivo de texto antes de eliminarla.

Administración de políticas mediante la API de Amazon SES

La administración de las políticas de Amazon SES permite visualizar, editar o eliminar una política asociada a una identidad mediante la API de Amazon SES.

Para enumerar y ver políticas mediante la API de Amazon SES

- Puede mostrar las políticas que se han asociado a una identidad mediante la operación de la API ListIdentityPolicies. También puede recuperar las propias políticas mediante la operación de la API GetIdentityPolicies.

Para editar una política mediante la API de Amazon SES

- Puede editar una política que se ha adjuntado a una identidad mediante la operación de la API PutIdentityPolicy.

Para borrar una política mediante la API de Amazon SES

- Puede borrar una política que se ha adjuntado a una identidad mediante la operación de la API DeleteIdentityPolicy.

Uso de la autorización de envío con Amazon SES

Puede configurar Amazon SES para permitir que otros usuarios envíen correo electrónico desde las identidades de su propiedad (dominios o direcciones de correo electrónico) mediante sus propias

cuentas de Amazon SES. Con la característica autorización de envío, podrá mantener el control sobre sus identidades de modo que pueda cambiar o revocar los permisos en cualquier momento. Por ejemplo, si es el propietario de una compañía, puede usar la autorización de envío para permitir a un tercero (como una empresa de marketing por correo electrónico) enviar correo electrónico desde un dominio de su propiedad.

En este capítulo se describen las características específicas de la autorización de envío, que sustituye a la antigua función de notificaciones entre cuentas. En primer lugar, debe comprender los conceptos básicos de la autorización basada en la identidad mediante el uso de políticas de autorización, tal como se explica en Uso de la autorización de identidad en Amazon SES que aborda temas importantes, como la estructura de una política de autorización y la forma de administrar las políticas.

Soporte heredado de notificaciones entre cuentas

Las notificaciones de valoración de rebotes, reclamos y entregas asociadas con el correo electrónico enviado desde un remitente delegado, autorizado por un propietario de identidad para enviar desde una de sus identidades verificadas, se han configurado tradicionalmente mediante notificaciones entre cuentas en las que el remitente delegado asociaría un tema con una identidad de la que no era propietario (es decir, entre cuentas). Sin embargo, las notificaciones entre cuentas se han sustituido por el uso de conjuntos de configuración e identidades verificadas en asociación con el envío delegado, en el que el propietario de la identidad ha autorizado al remitente delegado para usar una de sus identidades verificadas desde las que enviar correos electrónicos. Este nuevo método permite la flexibilidad de configurar notificaciones de rebote, reclamo, entrega y otros eventos mediante los siguientes dos componentes fijos, dependiendo de si es el remitente delegado o el propietario de la identidad verificada:

- Conjuntos de configuración: el remitente delegado puede configurar la publicación de eventos en su propio conjunto de configuración que puede especificar al enviar un correo electrónico desde una identidad verificada que no le pertenece, pero desde la que el propietario ha autorizado envíos a través de una política de autorización. La publicación de eventos permite publicar notificaciones de rebotes, quejas, entregas y otros eventos en Amazon CloudWatch, Amazon Data Firehose, Amazon Pinpoint y Amazon SNS. Consulte Crear destinos de eventos.
- Identidades verificadas: además de que el propietario de la identidad autorice al remitente delegado el uso de una de sus identidades verificadas para enviar correos electrónicos, también puede, a petición del remitente delegado, configurar notificaciones de valoraciones sobre la identidad compartida para utilizar temas de SNS propiedad del remitente delegado. Solo el remitente delegado recibirá estas notificaciones porque es propietario del tema de SNS. Consulte

el paso 14 para obtener información sobre cómo configurar un "SNS topic you don't own" (Tema de SNS que no le pertenece) en los procedimientos de la política de autorización.

> **Note**
>
> Para fines de compatibilidad, se soportan notificaciones entre cuentas para las notificaciones entre cuentas heredadas que se están utilizando actualmente en su cuenta. Este soporte se limita a poder modificar y utilizar la opción entre cuentas actuales que haya creado en la consola clásica de Amazon SES; sin embargo, ya no puede crear nuevas notificaciones entre cuentas. Para crear otras nuevas opciones en la nueva consola de Amazon SES, utilice los nuevos métodos de envío delegado con conjuntos de configuración mediante publicación de eventos, o con identidades verificadas configuradas con sus propios temas de SNS.

Temas

- Información general de la autorización de envío de Amazon SES
- Tareas de propietario de identidad para autorización de envío de Amazon SES
- Tareas de remitente delegado para la autorización de envío de Amazon SES

Información general de la autorización de envío de Amazon SES

En este tema, se proporciona información general acerca del proceso de autorización de envío y, a continuación, se explica cómo las características de envío de correo electrónico de Amazon SES, tales como las cuotas de envío y las notificaciones, funcionan con la autorización de envío.

En esta sección, se usan los siguientes términos:

- Identidad: dirección o dominio de correo electrónico que los usuarios de Amazon SES utilizan para enviar correo electrónico.
- Propietario de identidad: un usuario de Amazon SES cuya propiedad de dirección o dominio de correo electrónico se ha verificado utilizando el procedimiento descrito en Identidades verificadas.
- Remitente delegado: una cuenta de AWS, un usuario de AWS Identity and Access Management(IAM) o un servicio de AWS autorizado mediante una política de autorización para enviar correos electrónicos en nombre del propietario de la identidad.
- Política de autorización de envío: un documento que adjunta a una identidad para especificar quién puede realizar envíos para esa identidad y en qué condiciones.

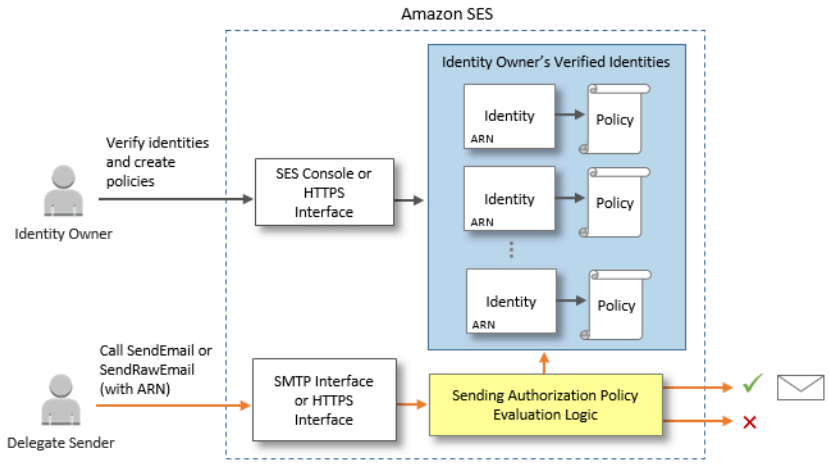
- Nombre de recurso de Amazon (ARN): una forma estandarizada de identificar de manera inequívoca un recurso de AWS en todos los servicios de AWS. Para la autorización de envío, el recurso es la identidad que el propietario de la identidad ha autorizado al remitente delegado a utilizar. Un ejemplo de ARN es arn:aws:ses:us-east-1:123456789012:identity/example.com.

Proceso de autorización de envío

La autorización de envío se basa en políticas de autorización de envío. Si desea habilitar un remitente delegado para que realice envíos en su nombre, debe crear una política de autorización de envío y asociar la política a su identidad a través de la consola de Amazon SES o la API de Amazon SES. Cuando el remitente delegado intenta enviar un correo electrónico a través de Amazon SES en su nombre, el remitente delegado transfiere el ARN de su identidad en la solicitud o en el encabezado del correo electrónico.

Cuando Amazon SES recibe la solicitud para enviar el correo electrónico, comprueba la política de su identidad (si la hay) a fin de determinar si ha autorizado al remitente delegado para enviar en nombre de la identidad. Si el remitente delegado está autorizado, Amazon SES acepta el correo electrónico; en caso contrario, devuelve un mensaje de error.

En el siguiente diagrama se muestra la relación de alto nivel entre los conceptos de autorización de envío:



El proceso de autorización de envío consta de los siguientes pasos:

1. El propietario de la identidad selecciona una identidad verificada para que la utilice el remitente delegado. (Si no ha verificado una identidad, consulte Identidades verificadas).

> **Note**
>
> La identidad verificada que elija para el remitente delegado no puede tener un conjunto de configuración predeterminado asignado a ella.

2. El remitente delegado informa al propietario de la identidad qué ID de cuenta de AWS o ARN de usuario de IAM desea utilizar para el envío.
3. Si el propietario de identidad acepta permitir al remitente delegado el envío desde una de las cuentas del propietario, el propietario crea una política de autorización de envío y asocia la política a la identidad elegida mediante la consola de Amazon SES o la API de Amazon SES.
4. El propietario de identidad ofrece el remitente delegado el ARN de la identidad autorizada, de modo que el remitente delegado puede proporcionar el ARN a Amazon SES en el momento en que se envía el correo electrónico.
5. El remitente delegado puede configurar notificaciones de rebotes y reclamos a través de la habilitación de publicación de eventos en el conjunto de configuración especificado durante el envío delegado. El propietario de la identidad también puede configurar notificaciones de valoración por correo electrónico para los eventos de rebotes y reclamos que se enviarán a los temas de Amazon SNS del remitente delegado.

   > **Note**
   >
   > Si el propietario de la identidad desactiva el envío de notificaciones de eventos, el remitente delegado debe configurar la publicación de eventos para publicar los eventos de rebote y queja en un tema de Amazon SNS o en una transmisión de Firehose. El remitente debe aplicar también el conjunto de configuración que contiene la regla de publicación de eventos a cada mensaje de correo electrónico que envíe. Si ni el propietario de identidad ni el remitente delegado configuran un método de envío de notificaciones para eventos de rebotes y reclamos, Amazon SES envía automáticamente notificaciones de eventos por correo electrónico a la dirección que figura en el campo Return-Path del mensaje (o a la dirección del campo Source, si no se ha especificado una dirección Return-Path), aunque el propietario de identidad haya desactivado el reenvío de retroalimentación de correo electrónico.
6. El remitente delegado intenta enviar un correo electrónico a través de Amazon SES en nombre del propietario de identidad al transferir el ARN de la identidad del propietario de identidad en la solicitud o en el encabezado del correo electrónico. El remitente delegado puede enviar el correo

electrónico mediante la interfaz de SMTP de Amazon SES o la API de Amazon SES. Tras recibir la solicitud, Amazon SES examina las políticas que se han asociado a la identidad y acepta el correo electrónico si el remitente delegado está autorizado para utilizar la dirección de remitente "From" especificada y la dirección de ruta de retorno "Return Path"; de lo contrario, Amazon SES devuelve un error y no acepta el mensaje.

> **Important**
>
> La cuenta de AWS del remitente delegado se debe eliminar del entorno aislado antes de que se pueda utilizar para enviar correo electrónico a direcciones no verificadas.

7. Si el propietario de identidad necesita anular la autorización del remitente delegado, deberá editar la política de autorización de envío o eliminar la política en su totalidad. El propietario de identidad puede realizar ambas acciones a través de la consola de Amazon SES o la API de Amazon SES.

Para obtener más información acerca de cómo el propietario de la identidad o el remitente delegado realizan estas tareas, consulte Tareas del propietario de identidad o Tareas del remitente delegado, respectivamente.

Atribución de características de envío de correo electrónico

Es importante entender el rol del remitente delegado y del propietario de identidad con respecto a las características de envío de correo electrónico de Amazon SES, tales como la cuota de envío diaria, los rebotes y reclamos, la firma de DKIM, el reenvío de retroalimentación, etc. La atribución es la siguiente:

- Cuotas de envío: el correo electrónico enviado desde las identidades del propietario de identidad se contabiliza en las cuotas del remitente.
- Rebotes y reclamo: los eventos de rebotes y reclamos se contabilizan en la cuenta de Amazon SES del remitente y, por tanto, afectan a la reputación del remitente delegado.
- Firma de DKIM: si el propietario de identidad ha habilitado la firma de Easy DKIM para una identidad, todo el correo electrónico enviado desde dicha identidad estará firmado por DKIM, incluido el correo electrónico enviado por el remitente delegado. Solo el propietario de identidad puede controlar si los correos electrónicos están firmados con DKIM.
- Notificaciones: el propietario de identidad y el remitente delegado pueden configurar notificaciones para rebotes y reclamos. El propietario de la identidad de correo electrónico también puede

habilitar el reenvío de retroalimentación de correo electrónico. Para obtener información sobre la configuración de notificaciones, consulte Monitoreo de la actividad de envío de Amazon SES.

- Verificación: los propietarios de identidad son responsables de realizar el procedimiento que se describe en Identidades verificadas para verificar que son los propietarios de las direcciones de correo electrónico y de los dominios cuyo uso autorizan a los remitentes delegados. Los remitentes delegados no tienen que comprobar ninguna dirección de correo electrónico o dominios específicamente para la autorización de envío.

  > **Important**
  >
  > La cuenta de AWS del remitente delegado se debe eliminar del entorno aislado antes de que se pueda utilizar para enviar correo electrónico a direcciones no verificadas.

- Regiones de AWS: el remitente delegado debe enviar los mensajes de correo electrónico desde la región de AWS en la que se verifica la identidad del propietario de identidad. La política de autorización de envío que otorga permiso al remitente delegado debe estar asociada a la identidad en dicha región.
- Facturación: todos los mensajes que se envían desde la cuenta del remitente delegado, incluidos los correos electrónicos que este envía utilizando las direcciones del propietario de la identidad, se facturan al remitente delegado.

Tareas de propietario de identidad para autorización de envío de Amazon SES

En esta sección, se describen los pasos que los propietarios de identidad deben realizar al configurar la autorización de envío.

Temas

- Verificación de una identidad para autorización de envío de Amazon SES
- Configuración de notificaciones de propietario de identidad para autorización de envío de Amazon SES
- Obtención de información del remitente delegado para la autorización de envío de Amazon SES
- Creación de una política de autorización de envío en Amazon SES
- Ejemplos de políticas de envío
- Proporcionar al remitente delegado la información de identidad para la autorización de envío de Amazon SES

Verificación de una identidad para autorización de envío de Amazon SES

El primer paso para configurar la autorización de envío es demostrar que usted es el propietario de la dirección de correo electrónico o el dominio que el remitente delegado usará para enviar correo electrónico. El procedimiento de verificación se describe en Identidades verificadas.

Puede confirmar que una dirección o dominio de correo electrónico se ha verificado al comprobar su estado en la sección Verified Identities (Identidades verificadas) de la https://console.aws.amazon.com/ses/ o mediante la operación de la API `GetIdentityVerificationAttributes`.

Antes de que usted o el remitente delegado puedan enviar correo electrónico a direcciones de correo electrónico no verificadas, debe enviar una solicitud para que su cuenta se elimine del entorno de pruebas de Amazon SES. Para obtener más información, consulte Solicitar acceso a la producción (salir del entorno de pruebas de Amazon SES) .

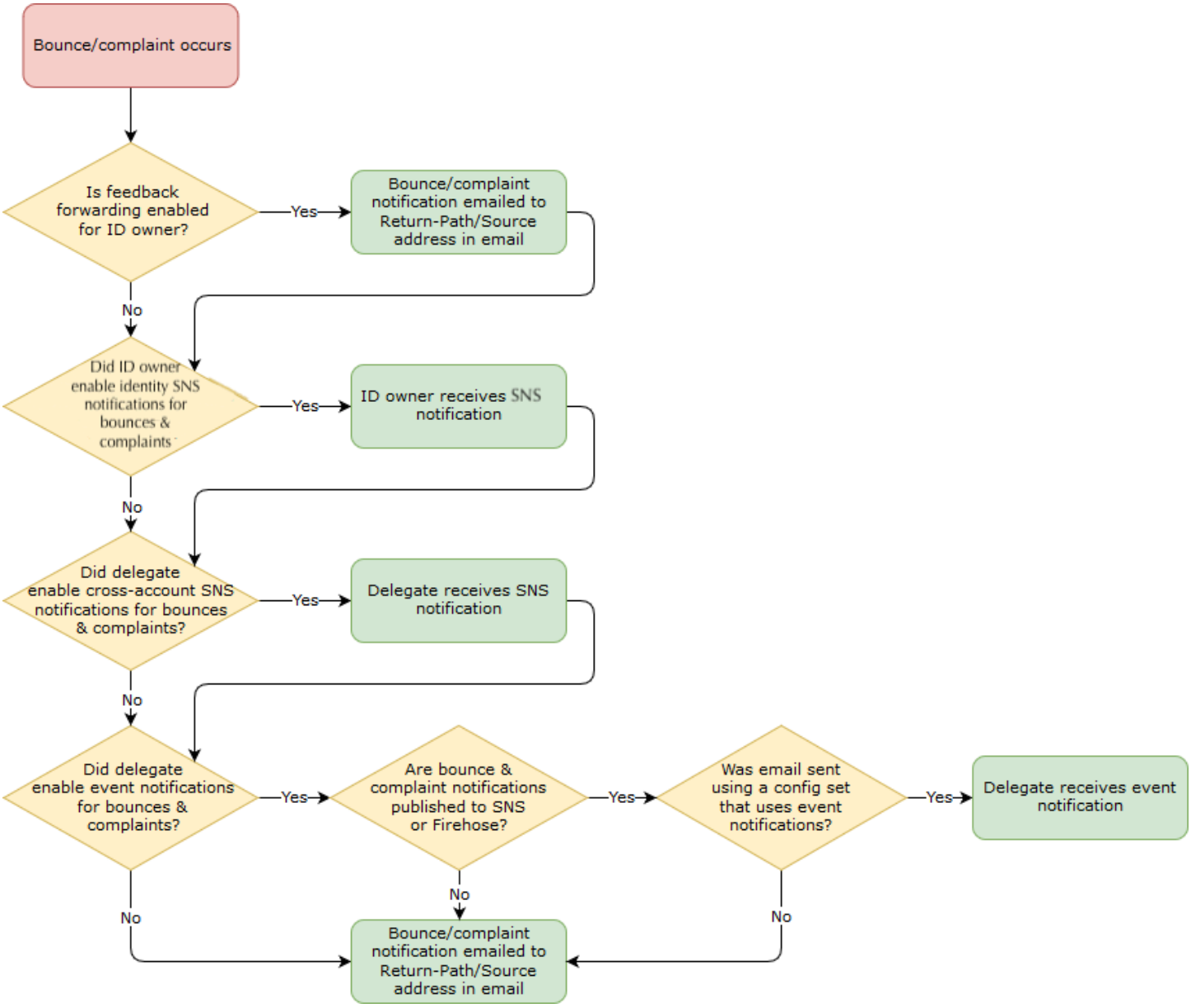
> **Important**
>
> La Cuenta de AWS del remitente delegado se debe eliminar del entorno aislado antes de que se pueda utilizar para enviar correo electrónico a direcciones no verificadas.

Configuración de notificaciones de propietario de identidad para autorización de envío de Amazon SES

Si autoriza a un remitente delegado a enviar correo electrónico en su nombre, Amazon SES contabiliza todos los rebotes o reclamos que generan dichos correos electrónicos en los límites de rebotes y reclamos del remitente delegado en lugar de en los de usted. Sin embargo, si su dirección IP figura en listas negras basadas en DNS antispam de terceros (DNSBL) como resultado de los mensajes enviados por un remitente delegado, la reputación de esas identidades puede deteriorarse. Por este motivo, si usted es propietario de identidades, debería configurar el reenvío de valoraciones de correo electrónico para todas sus identidades, incluso las que ha autorizado para el envío delegado. Para obtener más información, consulte Recepción de notificaciones de Amazon SES por correo electrónico.

Los remitentes delegados pueden y deben configurar sus propias notificaciones de rebotes y reclamos para las identidades cuyo uso se les ha autorizado. Pueden configurar la publicación de eventos para publicar eventos de rebote y queja en un tema de Amazon SNS o en una transmisión de Firehose.

Si ni el propietario de identidad ni el remitente delegado configuran un método de envío de notificaciones para eventos de rebotes y reclamos, o si el remitente no aplica el conjunto de configuración que utiliza la regla de publicación de eventos, Amazon SES envía automáticamente notificaciones de eventos por correo electrónico a la dirección que figura en el campo Return-Path del mensaje (o a la dirección del campo Source, si no se ha especificado una dirección Return-Path), aunque se haya desactivado el reenvío de retroalimentación de correo electrónico. Este proceso se ilustra en la imagen siguiente.



Obtención de información del remitente delegado para la autorización de envío de Amazon SES

Su política de autorización de envío debe especificar al menos una entidad principal, que es la entidad del remitente delegado al que está concediendo acceso para que pueda enviar en nombre

de una de sus identidades verificadas. Para las políticas de autorización de envío de Amazon SES, la entidad principal puede ser su cuenta de AWS de remitente delegado o ARN de usuario de AWS Identity and Access Management (IAM) o un servicio de AWS.

Una forma de considerar esto es que la entidad principal (remitente delegado) es el beneficiario, y usted (propietario de la identidad) es el otorgante en la política de autorización en la que le concede el permiso, Permitir, para enviar cualquier combinación de correo electrónico, correo electrónico sin procesar, correo electrónico con plantilla o correo electrónico con plantilla masiva desde el recurso (identidad verificada) que le pertenece.

Si desea un control más detallado, solicite al remitente delegado que configure un usuario de IAM de modo que solo un remitente delegado pueda enviarle correo electrónico a usted en lugar de cualquier usuario de la cuenta de AWS del remitente delegado. El remitente delegado encontrará información acerca de la configuración de un usuario de IAM en Creación de un usuario de IAM en su cuenta de AWS en la Guía del usuario de IAM.

Solicite a su remitente delegado el ID de cuenta de AWS o el nombre de recurso de Amazon (ARN) del usuario de IAM para incluirlo en su política de autorización de envío. Puede remitir a su remitente delegado a las instrucciones para buscar esta información en Proporcionar información al propietario de identidad. Si el remitente delegado es un servicio de AWS, consulte la documentación correspondiente a dicho servicio para determinar el nombre del servicio.

En el siguiente ejemplo de política se ilustran los elementos básicos necesarios en una política creada por el propietario de la identidad para autorizar al remitente delegado a enviar desde el recurso del propietario de identidad. El propietario de la identidad entraría en el flujo de trabajo de Verified identities (Identidades verificadas) y, en Authorization (Autorización) utilizaría el Policy generator (Generador de políticas) para crear, en su forma más sencilla, la siguiente política básica que permita al remitente delegado enviar en nombre de un recurso del propietario de la identidad:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "stmt1632010098378",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "ses:SendEmail",
                "ses:SendRawEmail"
            ],
            "Resource": "arn:aws:ses:us-east-1:444455556666:identity/bob@example.com",
            "Condition": {}
        }
    ]
}
```

Para la política anterior, en la siguiente leyenda se explican los elementos clave y quién es el propietario:

- Entidad principal: este campo se rellena con el ARN de usuario de IAM del remitente delegado.
- Acción: este campo se rellena con dos acciones de SES (`SendEmail` y `SendRawEmail`) que el propietario de identidad permite que el remitente delegado realice desde el recurso del propietario de identidad.
- Recurso: este campo se rellena con el recurso verificado del propietario de identidad desde el que autoriza al remitente delegado el envío.

Creación de una política de autorización de envío en Amazon SES

De forma similar a la creación de una política de autorización en Amazon SES, tal como se explica en Creación de una política de autorización de identidad, para autorizar a un remitente delegado a enviar correos electrónicos con una dirección de correo electrónico o un dominio (una identidad) de su propiedad, debe crear una política especificando las acciones de la API de envío de SES y, a continuación, asociar dicha política a la identidad.

Para obtener una lista de las acciones de la API que se pueden especificar en una política de autorización de envío, consulte la fila Acción de la tabla the section called “Instrucciones específicas de la política”.

Puede crear una política de autorización de envío mediante el generador de políticas o mediante la creación de una política personalizada. Se proporcionan procedimientos específicos para crear una política de autorización de envío para cualquiera de los métodos.

> **Note**
>
> - Las políticas de autorización de envío que asocia a identidades de direcciones de correo electrónico prevalecen sobre las políticas que asocia a sus identidades de dominio correspondientes. Por ejemplo, si crea una política para example.com que deshabilita a un remitente delegado y crea una política para sender@example.com que habilita al remitente delegado, el remitente delegado podrá enviar correos electrónicos desde sender@example.com, pero no desde cualquier otra dirección del dominio example.com.
> - Si crea una política para example.com que permita a un remitente delegado y crea una política para sender@example.com que no permite al remitente delegado, el remitente delegado puede enviar correo electrónico desde cualquier dirección del dominio example.com excepto sender@example.com.
> - Si no está familiarizado con la estructura de las políticas de autorización de SES, consulteAnatomía de las políticas.

Creación de una política de autorización de envío mediante el generador de políticas

Puede usar el generador de políticas para crear una política de autorización de envío mediante los pasos que se indican a continuación.

Para crear una política de autorización de envío mediante el generador de políticas

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).
3. En el contenedor Identities (Identidades) en la pantalla Verified identities (Identidades verificadas), seleccione la identidad verificada que desea autorizar para que el remitente delegado envíe en su nombre.
4. Elija la pestaña Autorización de la identidad verificada.
5. En el panel Authorization policies (Políticas de autorización), elija Create policy (Crear política) y seleccione Use policy generator (Utilizar generador de políticas) en el menú desplegable.

6. En el panel Create statement (Crear instrucción), elija Allow (Permitir) en el campo Effect (Efecto). (Si desea crear una política para restringir al remitente delegado, elija Deny [Rechazar] en su lugar.)
7. En el campo Principals (Entidades principales), introduzca el ID de Cuenta de AWS o ARN de usuario de IAM que el remitente delegado compartió con usted para autorizar el envío de correos electrónicos en nombre de su cuenta para esta identidad y, a continuación, elija Add (Agregar). (Si desea autorizar a más de un remitente delegado, repita este paso para cada uno).
8. En el campo Actions (Acciones), marque la casilla de verificación de cada tipo de envío que desea autorizar para su remitente delegado.
9. (Opcional) Expanda Specify conditions (Especificar condiciones) si desea agregar una instrucción calificada al permiso del remitente delegado.
    a. Seleccione un operador de la lista desplegable Operator (Operador).
    b. Seleccione un tipo de la lista desplegable Key (Clave).
    c. Respecto del tipo de clave que ha seleccionado, introduzca su valor en el campo Value (Valor). (Si desea agregar más condiciones, elija Add new condition [Agregar nueva condición] y repita este paso para cada condición adicional.)
10. Elija Save statement (Guardar instrucción).
11. (Opcional) Expanda Create another statement (Crear otra instrucción) si desea agregar más instrucciones a su política y repita los pasos 6 a 10.
12. Elija Next (Siguiente) y, en la pantalla Customize policy (Personalizar política), el contenedor Edit policy details (Editar detalles de la política) incluye campos en los que puede cambiar o personalizar el Name (Nombre) y el Policy document (Documento de la política).
13. Elija Next (Siguiente) y en la pantalla Review and apply (Revisar y aplicar), el contenedor Overview (Información general) mostrará la identidad verificada que está autorizando para su remitente delegado, así como el nombre de esta política. En el panel Policy document (Documento de la política) encontrará la política real que acaba de escribir junto con cualquier condición que haya agregado: revise la política y, si parece correcta, elija Apply policy (Aplicar política). (Si necesita cambiar o corregir algo, elija Previous [Anterior] y trabaje en el contenedor Edit policy details [Editar detalles de la política]. La política que acaba de crear permitirá a su remitente delegado enviar en su nombre.
14. (Opcional) Si el remitente delegado también quiere utilizar un tema de SNS de su propiedad, recibir notificaciones de valoraciones cuando recibe rebotes o reclamos, o cuando se entregan correos electrónicos, deberá configurar su tema de SNS en esta identidad verificada. (El

remitente delegado tendrá que compartir con usted su ARN de tema de SNS). Seleccione la pestaña Notifications (Notificaciones) y seleccione Edit (Editar) en el contenedor Feedback notifications (Notificaciones de valoración):

a. En el panel Configure SNS topics (Configurar temas de SNS), en cualquiera de los campos de valoración, (Rebote, Reclamo o Entrega), seleccione SNS topic you don't own (Tema de SNS del que no es propietario) e introduzca el SNS topic ARN (ARN del tema de SNS) propiedad de su remitente delegado, compartido con usted. (Solo el remitente delegado recibirá estas notificaciones porque es propietario del tema de SNS; usted, como propietario de la identidad, no lo hará).

b. (Opcional) Si desea que la notificación del tema incluya los encabezados del correo electrónico original, marque la casilla Include original email headers (Incluir encabezados de correo electrónico originales) directamente debajo del nombre del tema de SNS de cada tipo de valoración. Esta opción solo está disponible si ha asignado un tema de Amazon SNS al tipo de notificación asociado. Para obtener información sobre el contenido de los encabezados de correo electrónico originales, consulte el objeto `mail` en Contenido de las notificaciones.

c. Elija Save changes (Guardar cambios). Los cambios que haya realizado en su configuración de notificaciones podrían tardar varios minutos en surtir efecto.

d. (Opcional) Dado que el remitente delegado recibirá notificaciones de temas de Amazon SNS para rebotes y reclamos, puede desactivar por completo las notificaciones por correo electrónico si no quiere recibir valoraciones sobre los envíos de esta identidad. Para desactivar las valoraciones por correo electrónico de rebotes y reclamos, en la pestaña Notifications (Notificaciones) en el contenedor Email Feedback Forwarding (Reenvío de valoración de correo), elija Edit (Editar), desmarque la casilla Enabled (Habilitado), y elija Save changes (Guarde los cambios). Ahora, las notificaciones de estado de entrega solo se enviarán a los temas de SNS propiedad de su remitente delegado.

Creación de una política de autorización de envío personalizada

Si desea crear una política de autorización de envío personalizada y asociarla a una identidad, dispone de las siguientes opciones:

- Mediante la API de Amazon SES: cree una política en un editor de texto y, a continuación, adjúntela a la identidad a través de la API de `PutIdentityPolicy`, que se describe en la Referencia de la API de Amazon Simple Email Service.

- Mediante la consola de Amazon SES: cree una política en un editor de texto y adjúntela a una identidad pegándola en el editor de políticas personalizadas en la consola de Amazon SES. El siguiente procedimiento describe este método.

Para crear una política de autorización de envío personalizada mediante el editor de políticas personalizadas

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).
3. En el contenedor Identities (Identidades) en la pantalla Verified identities (Identidades verificadas), seleccione la identidad verificada que desea autorizar para que el remitente delegado envíe en su nombre.
4. En la pantalla de detalles de la identidad verificada que seleccionó en el paso anterior, elija la pestaña Authorization (Autorización).
5. En el panel Authorization policies (Políticas de autorización), elija Create policy (Crear política) y seleccione Create custom policy (Crear política personalizada) en el menú desplegable.
6. En el panel Policy document (Documento de la política), pegue el texto de su política en formato JSON. También puede usar el generador de políticas para crear rápidamente la estructura básica de una política y, a continuación, personalizarla aquí.
7. Seleccione Apply Policy. (Si alguna vez necesita modificar su política personalizada, marque la casilla de verificación debajo de la pestaña Authorization [Autorización], elija Edit [Editar] y realice los cambios en el panel Policy document (Documento de la política), seguido de Save changes [Guardar los cambios]).
8. (Opcional) Si el remitente delegado también quiere utilizar un tema de SNS de su propiedad, recibir notificaciones de valoraciones cuando recibe rebotes o reclamos, o cuando se entregan correos electrónicos, deberá configurar su tema de SNS en esta identidad verificada. (El remitente delegado tendrá que compartir con usted su ARN de tema de SNS). Seleccione la pestaña Notifications (Notificaciones) y seleccione Edit (Editar) en el contenedor Feedback notifications (Notificaciones de valoración):

    a. En el panel Configure SNS topics (Configurar temas de SNS), en cualquiera de los campos de valoración, (Rebote, Reclamo o Entrega), seleccione SNS topic you don’t own (Tema de SNS del que no es propietario) e introduzca el SNS topic ARN (ARN del tema de SNS)

propiedad de su remitente delegado, compartido con usted. (Solo el remitente delegado recibirá estas notificaciones porque es propietario del tema de SNS; usted, como propietario de la identidad, no lo hará).

b. (Opcional) Si desea que la notificación del tema incluya los encabezados del correo electrónico original, marque la casilla Include original email headers (Incluir encabezados de correo electrónico originales) directamente debajo del nombre del tema de SNS de cada tipo de valoración. Esta opción solo está disponible si ha asignado un tema de Amazon SNS al tipo de notificación asociado. Para obtener información sobre el contenido de los encabezados de correo electrónico originales, consulte el objeto `mail` en Contenido de las notificaciones.

c. Elija Save changes (Guardar cambios). Los cambios que haya realizado en su configuración de notificaciones podrían tardar varios minutos en surtir efecto.

d. (Opcional) Dado que el remitente delegado recibirá notificaciones de temas de Amazon SNS para rebotes y reclamos, puede desactivar por completo las notificaciones por correo electrónico si no quiere recibir valoraciones sobre los envíos de esta identidad. Para desactivar las valoraciones por correo electrónico de rebotes y reclamos, en la pestaña Notifications (Notificaciones) en el contenedor Email Feedback Forwarding (Reenvío de valoración de correo), elija Edit (Editar), desmarque la casilla Enabled (Habilitado), y elija Save changes (Guarde los cambios). Ahora, las notificaciones de estado de entrega solo se enviarán a los temas de SNS propiedad de su remitente delegado.

Ejemplos de políticas de envío

La autorización de envío le permite especificar las condiciones detalladas según las cuales permite a los remitentes delegados enviar en su nombre.

Los siguientes ejemplos y condiciones muestran cómo escribir políticas para controlar distintos aspectos de envío:

- Condiciones específicas para la autorización de envío
- Especificación del remitente delegado
- Restricción de la dirección de remitente (“From”)
- Restricción del periodo de tiempo en el que el delegado puede enviar correo electrónico
- Restricción de la acción de envío de correo electrónico
- Restricción del nombre de visualización del remitente de correo electrónico
- Uso de varias instrucciones

Condiciones específicas para la autorización de envío

Una condición es cualquier restricción sobre el permiso en la instrucción. La parte de la instrucción que especifica las condiciones puede ser la más detallada de todas las partes. Una clave es la característica específica que es la base para la restricción de acceso, como la fecha y hora de la solicitud.

Las condiciones y las claves se utilizan conjuntamente para expresar la restricción. Por ejemplo, si desea impedir que el remitente delegado realice solicitudes a Amazon SES en su nombre después del 30 de julio de 2019, utilice la condición denominada `DateLessThan`. Usted utiliza la clave denominada `aws:CurrentTime` y la define con el valor `2019-07-30T00:00:00Z`.

Puede utilizar cualquiera de las claves de escala de AWS que aparecen en Claves disponibles en la Guía del usuario de IAM o puede utilizar una de las siguientes claves específicas de SES que son muy útiles en las políticas de autorización de envío:

Clave de condición	Descripción
`ses:Recipients`	Restringe las direcciones del destinatario, que incluyen las direcciones To:, "CC" y "BCC".
`ses:FromAddress`	Restringe la dirección de remitente ("From").
`ses:FromDisplayName`	Restringe el contenido de la cadena que se utiliza como el nombre de visualización "From" (a veces denominado "remitente descriptivo"). Por ejemplo, el nombre de visualización de "John Doe <johndoe@example.com>" es John Doe.
`ses:FeedbackAddress`	Restringe la dirección de "ruta de retorno", que es la dirección donde se pueden enviar los rebotes y reclamaciones mediante reenvío de retroalimentación de correo electrónico. Para obtener información acerca del reenvío de retroalimentación de correo electrónico, consulte Recepción de notificaciones de Amazon SES por correo electrónico.

Puede utilizar las condiciones `StringEquals` y `StringLike` con claves de Amazon SES. Las condiciones son para coincidencia de cadenas con distinción entre mayúsculas y minúsculas. Para `StringLike`, los valores pueden incluir un comodín de coincidencias de varios caracteres (*) o un comodín de coincidencia de un único carácter (?) en cualquier parte de la cadena. Por ejemplo, la siguiente condición especifica que el remitente delegado solo puede enviar desde una dirección de remitente ("From") que empieza por invoicing y termina por @example.com:

```
"Condition": {
    "StringLike": {
      "ses:FromAddress": "invoicing*@example.com"
    }
}
```

También puede utilizar la condición `StringNotLike` para evitar que los remitentes delegados envíen correo electrónico desde determinadas direcciones de correo electrónico. Por ejemplo, puede deshabilitar el envío desde admin@example.com y direcciones similares como "admin"@example.com, admin+1@example.com o sender@admin.example.com al incluir la siguiente condición en su instrucción de política:

```
"Condition": {
    "StringNotLike": {
      "ses:FromAddress": "*admin*example.com"
    }
 }
```

Para obtener más información acerca de cómo especificar condiciones, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

Especificación del remitente delegado

La entidad principal, que es la entidad a la que se conceden los permisos, puede ser una cuenta de Cuenta de AWS, un usuario de AWS Identity and Access Management (IAM) o un servicio de AWS.

El siguiente ejemplo muestra una política sencilla que permite al ID de AWS 123456789012 enviar correo electrónico desde la identidad verificada example.com (que es propiedad de Cuenta de AWS 888888888888). La instrucción `Condition` de esta política solo permite al delegado (es decir, el ID de AWS 123456789012) enviar correo electrónico desde la dirección marketing+.*@example.com, donde * es cualquier cadena que el remitente quiera agregar después de marketing+.

```
{
```

```
  "Id":"SampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeMarketer",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition":{
        "StringLike":{
          "ses:FromAddress":"marketing+.*@example.com"
        }
      }
    }
  ]
}
```

La siguiente política de ejemplo otorga a dos usuarios de IAM permiso para enviar desde la identidad example.com. Los usuarios de IAM se especifican por su nombre de recurso de Amazon (ARN).

```
{
  "Id":"ExampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeIAMUser",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "AWS":[
          "arn:aws:iam::111122223333:user/John",
          "arn:aws:iam::444455556666:user/Jane"
        ]
      },
      "Action":[
```

```
        "ses:SendEmail",
        "ses:SendRawEmail"
      ]
    }
  ]
}
```

La siguiente política de ejemplo otorga a Amazon Cognito permiso para enviar desde la identidad example.com.

```
{
  "Id":"ExampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeService",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "Service":[
          "cognito-idp.amazonaws.com"
        ]
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "888888888888",
          "aws:SourceArn": "arn:aws:cognito-idp:us-east-1:888888888888:userpool/your-
user-pool-id-goes-here"
        }
      }
    }
  ]
}
```

La siguiente política de ejemplo otorga permiso a todas las cuentas dentro de una organización de AWS para enviar desde la identidad example.com. La organización de AWS se especifica mediante la clave de condición global PrincipalOrgID.

```
{
  "Id":"ExampleAuthorizationPolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeOrg",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":"*",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition":{
        "StringEquals":{
          "aws:PrincipalOrgID":"o-xxxxxxxxxx"
        }
      }
    }
  ]
}
```

Restricción de la dirección de remitente (“From”)

Si utiliza un dominio verificado, puede crear una política que permita únicamente a un remitente delegado enviar correo electrónico desde una dirección de correo electrónico especificada. Para restringir la dirección de remitente ("From"), se establece una condición en la clave denominada ses:FromAddress. La siguiente política permite al ID de Cuenta de AWS 123456789012 enviar correo electrónico desde la identidad example.com, pero solo desde la dirección de correo electrónico sender@example.com.

```
{
  "Id":"ExamplePolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeFromAddress",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
```

```
        ]
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition":{
        "StringEquals":{
          "ses:FromAddress":"sender@example.com"
        }
      }
    }
  ]
}
```

Restricción del periodo de tiempo en el que el delegado puede enviar correo electrónico

También puede configurar la política de autorización del remitente de forma que un remitente delegado solo pueda enviar correo electrónico a una hora determinada del día o en un determinado intervalo de fechas. Por ejemplo, si tiene previsto enviar su campaña de correo electrónico durante el mes de septiembre de 2021, puede utilizar la siguiente política para restringir la capacidad del delegado de enviar correo electrónico solo durante ese mes.

```
{
  "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"
        }
      }
    }
  ]
}
```

Restricción de la acción de envío de correo electrónico

Hay dos acciones que los remitentes pueden utilizar para enviar correo electrónico con Amazon SES: `SendEmail` y `SendRawEmail`, en función del control que el remitente desee tener sobre el formato del correo electrónico. Las políticas de autorización de envío le permiten limitar al remitente delegado a una de las dos acciones. Sin embargo, muchos propietarios de identidad habilitan ambas acciones en sus políticas, lo que permite que sea el remitente delegado quien decida los detalles de las llamadas de envío de correo electrónico.

> **Note**
>
> Si desea habilitar al remitente delegado para acceder a Amazon SES a través de la interfaz de SMTP, debe elegir `SendRawEmail` como mínimo.

Si su caso de uso es tal que desea restringir la acción, puede hacerlo incluyendo solo una de las acciones en su política de autorización de envío. El siguiente ejemplo muestra cómo restringir la acción a `SendRawEmail`.

```
{
  "Id":"ExamplePolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"ControlAction",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
```

```
      "Action":[
        "ses:SendRawEmail"
      ]
    }
  ]
}
```

Restricción del nombre de visualización del remitente de correo electrónico

Algunos clientes de correo electrónico muestran el nombre "descriptivo" del remitente de correo electrónico (si el encabezado de correo electrónico lo proporciona), en lugar de la dirección de remitente ("From") real. Por ejemplo, el nombre de visualización de "John Doe <johndoe@example.com>" es John Doe. Por ejemplo, podría enviar correos electrónicos desde user@example.com, pero prefiere que dichos destinatarios vean que el correo electrónico procede de marketing en lugar de user@example.com. La siguiente política permite al ID de Cuenta de AWS 123456789012 enviar correo electrónico desde la identidad example.com, pero solo si el nombre de visualización de la dirección del remitente (“From”) incluye Marketing.

```
{
  "Id":"ExamplePolicy",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeFromAddress",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:888888888888:identity/example.com",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition":{
        "StringLike":{
          "ses:FromDisplayName":"Marketing"
        }
      }
    }
  ]
```

```
}
```

Uso de varias instrucciones

La política de autorización de envío puede incluir varias instrucciones. La siguiente política de ejemplo contiene dos instrucciones. La primera instrucción permite que dos Cuentas de AWS distintas envíen correo electrónico desde sender@example.com, siempre y cuando la dirección del remitente (“From”) y la dirección de retroalimentación utilicen el dominio example.com. La segunda instrucción autoriza a un usuario de IAM a enviar correo electrónico desde sender@example.com siempre que la dirección de correo electrónico del destinatario esté en el dominio example.com.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AuthorizeAWS",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:999999999999:identity/sender@example.com",
      "Principal":{
        "AWS":[
          "111111111111",
          "222222222222"
        ]
      },
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition":{
        "StringLike":{
          "ses:FromAddress":"*@example.com",
          "ses:FeedbackAddress":"*@example.com"
        }
      }
    },
    {
      "Sid":"AuthorizeInternal",
      "Effect":"Allow",
      "Resource":"arn:aws:ses:us-east-1:999999999999:identity/sender@example.com",
      "Principal":{
        "AWS":"arn:aws:iam::333333333333:user/Jane"
      },
      "Action":[
```

```
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Condition":{
        "ForAllValues:StringLike":{
          "ses:Recipients":"*@example.com"
        }
      }
    }
  ]
}
```

Proporcionar al remitente delegado la información de identidad para la autorización de envío de Amazon SES

Después de crear su política de autorización de envío y asociarla a su identidad, puede proporcionar al remitente delegado el nombre de recurso de Amazon (ARN) de la identidad. El remitente delegado transferirá dicho ARN a Amazon SES en la operación de envío de correo electrónico o en el encabezado del correo electrónico. Para buscar el ARN de su identidad, siga los pasos que se describen a continuación.

Para buscar el ARN de una identidad

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).
3. En la lista de identidades, elija la identidad a la que asoció la política de autorización de envío.
4. En el panel Summary (Resumen), la segunda columna, Amazon Resource Name (ARN) [Nombre de recurso de Amazon (ARN)], contendrá el ARN de la identidad. Tendrá un aspecto similar a arn:aws:ses:us-east-1:123456789012:identity/user@example.com. Copie todo el ARN y proporciónelo a su remitente delegado.

Tareas de remitente delegado para la autorización de envío de Amazon SES

Como remitente delegado, enviará correos electrónicos en nombre de una identidad que no le pertenece, pero que está autorizado a utilizar. Aunque realice el envío en nombre del propietario de identidad, los rebotes y los reclamos se contabilizan en sus métricas de rebotes y reclamos de su cuenta de AWS y el número de mensajes enviados se contabiliza en su cuota de envío. Usted

también tiene la responsabilidad de solicitar los aumentos de cuota de envío que pueda necesitar para enviar correo electrónico del propietario de identidad.

Como remitente delegado, debe realizar las siguientes tareas:

- Proporcionar información al propietario de identidad
- Uso de notificaciones de remitente delegado
- Envío de correo electrónico para el propietario de la identidad

Proporcionar información al propietario de identidad para la autorización de envío de Amazon SES

Como remitente delegado, debe proporcionar al propietario de identidad su ID de cuenta de AWS o el nombre de recurso de Amazon (ARN) de usuario de IAM, ya que enviará correo electrónico en nombre del propietario de la identidad. El propietario de la identidad necesita la información de su cuenta para que pueda crear una política que le otorgue a usted permiso para realizar envíos desde una de las identidades verificadas.

Si desea utilizar sus propios temas de SNS, puede solicitar que el propietario de la identidad configure notificaciones de valoraciones para rebotes, reclamos o entregas que se enviarán a uno o varios de sus temas de SNS. Para ello, tendrá que compartir el ARN de su tema de SNS con el propietario de su identidad para que pueda configurar su tema de SNS en la identidad verificada desde la que le autoriza a enviar.

En los siguientes procedimientos se explica cómo encontrar la información de su cuenta y los ARN del tema de SNS para compartir con el propietario de su identidad.

Para encontrar el ID de su cuenta de AWS

1. Inicie sesión en la AWS Management Console en https://console.aws.amazon.com.
2. En la esquina superior derecha de la consola, expanda su nombre/número de cuenta y, a continuación, seleccione My Account (Mi cuenta) desde el menú desplegable.
3. Se abrirá la página Account settings (Configuración de la cuenta) y mostrará toda la información de su cuenta, incluido su ID de cuenta de AWS.

Para encontrar el ARN de su usuario de IAM

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en https://console.aws.amazon.com/iam/.

2. En el panel de navegación, seleccione Users.
3. En la lista de usuarios, elija el nombre de usuario. La sección Summary (Resumen) muestra el ARN de usuario de IAM. El ARN es similar al siguiente ejemplo: arn:aws:iam::123456789012:user/John.

Para encontrar el ARN de su tema de SNS

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En el panel de navegación, elija Topics (Temas).
3. En la lista de temas, se muestran los ARN del tema de SNS en la columna ARN. El ARN se parece al siguiente ejemplo:arn:aws:sns:us-east- 1:444455556666:mi-sns-topic.

Uso de notificaciones de remitente delegado para autorización de envío de Amazon SES

Como remitente delegado, enviará mensajes de correo electrónico en nombre de una identidad que no le pertenece, pero que está autorizado a utilizar; sin embargo, los rebotes y los reclamos siguen contando en sus métricas de rebotes y reclamos, no en las del propietario de la identidad.

Si la tasa de rebotes o de reclamos de su cuenta es demasiado alta, su cuenta corre el riesgo de someterse a revisión o de que se suspenda su capacidad para enviar correo electrónico. Por este motivo, es importante que configure las notificaciones y que disponga de un proceso para monitorizarlas. También debe contar con un proceso para eliminar de sus listas de correo las direcciones que generen rebotes o reclamaciones.

Por lo tanto, como remitente delegado, puede configurar Amazon SES para que envíe notificaciones cuando se produzcan eventos de rebote y reclamos para los mensajes de correo electrónico que envíe en nombre de cualquier identidad que no le pertenezca, pero que el propietario de la identidad lo haya autorizado a utilizar. También puedes configurar la publicación de eventos para publicar notificaciones de devoluciones y quejas en Amazon SNS o Firehose.

> **Note**
>
> Si configura Amazon SES para enviar notificaciones mediante Amazon SNS, se le cobrarán las tarifas estándar de Amazon SNS para las notificaciones que reciba. Para obtener más información, consulte la Página de precios de Amazon SNS.

Creación de una nueva notificación de remitente delegado

Puede configurar el envío delegado de notificaciones con conjuntos de configuración mediante la publicación de eventos o con identidades verificadas configuradas con sus propios temas de SNS.

A continuación se detallan los procedimientos para configurar nuevas notificaciones de envío delegado, mediante cualquiera de los métodos a continuación:

- Publicación de eventos mediante un conjunto de configuración
- Notificaciones de valoraciones a los temas de SNS que le pertenecen

Para configurar la publicación de eventos mediante un conjunto de configuración para el envío delegado

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. Siga los procedimientos indicados en Crear destinos de eventos.
3. Después de configurar la publicación de eventos en el conjunto de configuración, especifique el nombre del conjunto de configuración cuando envíe correo electrónico como remitente delegado mediante la identidad verificada desde la que el propietario de la identidad le autorizó a enviar. Consulte Envío de correo electrónico para el propietario de la identidad.

Para configurar notificaciones de valoraciones a los temas de SNS que le pertenecen para el envío delegado

1. Después de decidir cuál de los temas de SNS desea utilizar para las notificaciones de valoraciones, siga los procedimientos para encontrar el ARN de su tema de SNS y copie el ARN completo y compártalo con el propietario de su identidad.
2. Pídale al propietario de identidad que configure los temas de SNS para las notificaciones de valoraciones sobre la identidad compartida desde la que lo ha autorizado a enviar. (El propietario de identidad deberá seguir los procedimientos indicados para configuración de temas de SNS en los procedimientos de la política de autorización.)

Envío de correo electrónico al propietario de la identidad para la autorización de envío de Amazon SES

Como remitente delegado, envía correos electrónicos de la misma forma que lo hacen otros remitentes de Amazon SES, salvo que proporciona el Nombre de recurso de Amazon (ARN) de la identidad que el propietario de identidad lo ha autorizado a utilizar. Cuando llama a Amazon SES para enviar el correo electrónico, Amazon SES comprueba si la identidad que ha especificado tiene una política que lo autoriza a enviarlo.

Existen diferentes maneras en las que puede especificar el ARN de la identidad al enviar un correo electrónico. El método que puede utilizar depende de si envía el correo electrónico mediante las operaciones de la API de Amazon SES o la interfaz de SMTP de Amazon SES.

> **Important**
>
> Para enviar correctamente un correo electrónico, debe conectarse al punto de enlace de Amazon SES en la región de AWS en la que el propietario de identidad verificó la identidad. Además de las cuentas de AWS, el propietario de identidad y del remitente delegado deben eliminarse del entorno de pruebas para que cualquiera de las cuentas pueda enviar correo electrónico a direcciones no verificadas. Para obtener más información, consulte Solicitar acceso a la producción (salir del entorno de pruebas de Amazon SES) .

Uso de la API de Amazon SES

Al igual que con cualquier remitente de correo electrónico de Amazon SES, si accede a Amazon SES a través de la API de Amazon SES (ya sea directamente a través de HTTPS o indirectamente a través de un SDK de AWS), puede elegir entre una de las tres acciones de envío de correo electrónico: `SendEmail`, `SendTemplatedEmail` y `SendRawEmail`. En la Referencia de la API de Amazon Simple Email Service se describen los detalles de estas API, pero aquí ofrecemos información general de los parámetros de la autorización de envío.

SendRawEmail

Si desea utilizar `SendRawEmail` para poder controlar el formato de sus mensajes de correo electrónico, puede especificar la identidad autorizada delegada de alguna de las dos formas siguientes:

- Pasar parámetros opcionales a la API **`SendRawEmail`**. Los parámetros obligatorios se describen en la siguiente tabla:

Parámetro	Descripción
`SourceArn`	El ARN de la identidad que está asociada a la política de autorización de envío que le permite enviar para la dirección de correo electrónico especificada en el parámetro `Source` de `SendRawEmail` . **Note** Si solo especifica el `SourceArn` , Amazon SES establece la dirección del remitente ("From") y la dirección de la ruta de retorno ("Return Path") en la identidad especificada en `SourceArn` .
`FromArn`	El ARN de la identidad que está asociada a la política de autorización de envío que le permite especificar una dirección de remitente ("From") particular en el encabezado del correo electrónico sin procesar.
`ReturnPathArn`	El ARN de la identidad que está asociada a la política de autorización de envío que le permite utilizar la dirección de correo electrónico especificada en el parámetro `ReturnPath` de `SendRawEmail` .

- Incluir encabezados X en el correo electrónico. Los encabezados X son encabezados personalizados que puede utilizar además de los encabezados de correo electrónico estándar (como los encabezados From, Reply-To o Subject). Amazon SES reconoce tres encabezados X que puede utilizar para especificar parámetros de autorización de envío:

Important

No incluya estos encabezados X en la firma DKIM, ya que Amazon SES los elimina antes de enviar el correo electrónico.

Encabezado X	Descripción
X-SES-SOURCE-ARN	Corresponde a SourceArn .
X-SES-FROM-ARN	Corresponde a FromArn.
X-SES-RETURN-PATH-ARN	Corresponde a ReturnPathArn .

Amazon SES elimina todos los encabezados X del correo electrónico antes de enviarlo. Si se incluyen varias instancias de un encabezado X, Amazon SES solo utiliza la primera instancia.

El siguiente ejemplo muestra un correo electrónico que incluya encabezados X de autorización de envío:

```
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 y SendTemplatedEmail

Si utiliza la operación `SendEmail` o `SendTemplatedEmail`, puede especificar la identidad autorizada delegada al transferir los parámetros opcionales que se indican a continuación. No puede utilizar el método de encabezado X cuando utiliza la operación `SendEmail` o `SendTemplatedEmail`.

Parámetro	Descripción
`SourceArn`	El ARN de la identidad que está asociada a la política de autorización de envío que le permite enviar para la dirección de correo electrónico especificada en el parámetro `Source` de `SendEmail` o `SendTemplatedEmail`.
`ReturnPathArn`	El ARN de la identidad que está asociada a la política de autorización de envío que le permite utilizar la dirección de correo electrónico especificada en el parámetro `ReturnPath` de `SendEmail` o `SendTemplatedEmail`.

En el siguiente ejemplo, se muestra cómo enviar un correo electrónico que incluye los atributos `SourceArn` y `ReturnPathArn` mediante la operación `SendEmail` o `SendTemplatedEmail` y el SDK para 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'])
```

Uso de la interfaz de SMTP de Amazon SES

Cuando utilice la interfaz de SMTP de Amazon SES para el envío delegado, deberá incluir los encabezados `X-SES-SOURCE-ARN`, `X-SES-FROM-ARN` y `X-SES-RETURN-PATH-ARN` en el mensaje. Pase estos encabezados después enviar el comando `DATA` en la conversación SMTP.

Envío de correos electrónicos de prueba en Amazon SES con el simulador

Recomendamos utilizar la consola de Amazon SES para enviar un correo electrónico de prueba con Amazon SES. Dado que la consola requiere que introduzca manualmente información, normalmente solo la utiliza para enviar correos electrónicos de prueba. Después de comenzar a utilizar Amazon SES, lo más probable es que envíe los correos electrónicos a través de la API o de la interfaz de SMTP de Amazon SES. No obstante, la consola resulta útil para el monitoreo de la actividad de envío.

En los siguientes temas, se explica cómo utilizar el simulador de buzón de correo desde la consola y de forma manual mediante el envío de correos electrónicos:

- Uso del simulador de buzón de correo de la consola
- Uso del simulador de buzón de correo de forma manual

Uso del simulador de buzón de correo de la consola

> **Important**
>
> - En este tutorial, envíese un correo electrónico a usted mismo desde la consola para poder comprobar si lo recibe. Para seguir experimentando o cargar pruebas, consulte Uso del simulador de buzón de correo de forma manual.
> - Los correos electrónicos que envíe al simulador de bandeja de correo no se contabilizan en la cuota de envío ni en las tasas de rebotes y reclamaciones, ni afectan a las métricas de Virtual Deliverability Manager.

Antes de seguir estos pasos, realice las tareas de Configuración de Amazon Simple Email Service.

Para enviar un mensaje de correo electrónico de prueba desde la consola de Amazon SES

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Verified identities (Identidades verificadas).
3. Desde la tabla Identities (Identidades), seleccione una identidad de correo electrónico verificada (al hacer clic directamente en el nombre de la identidad en lugar de seleccionar su casilla de verificación). Si no dispone de una identidad de correo electrónico verificada, consulte Creación de una identidad de dirección de correo electrónico.
4. En la página de detalles de la identidad de correo electrónico seleccionada, elija Send test email (Enviar correo electrónico de prueba).
5. En Message details (Detalles del mensaje), elija una opción de Email Format (Formato de correo electrónico). Las dos opciones son las siguientes:

- Formatted (Con formato): se trata de la opción más sencilla. Seleccione esta opción si solo desea escribir el texto de su mensaje en el cuadro de texto Body. Al enviar el email, Amazon SES coloca el texto en formato de correo electrónico por usted.
- Raw (Sin formato): elija esta opción si desea enviar un mensaje más complejo, como, por ejemplo, un mensaje que incluya HTML o un archivo adjunto. Debido a esta flexibilidad, tiene que formatear el mensaje, tal y como se describe en Envío de correo electrónico sin procesar mediante la API v2 de Amazon SES, por sí mismo y, a continuación, pegar todo el mensaje con formato, incluidos los encabezados, en el cuadro de texto Body. Puede utilizar el siguiente ejemplo, que contiene HTML, para enviar un correo electrónico de prueba utilizando el formato de correo electrónico Raw. Copie y pegue este mensaje en su totalidad en el cuadro de texto Body. Asegúrese de que no haya ninguna línea en blanco entre el encabezado `MIME-Version` y el encabezado `Content-Type`; una línea en blanco entre estas dos líneas hace que el correo electrónico tenga formato de texto sin formato en lugar de 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. Amplíe el cuadro de lista Scenario (Escenario) para elegir el tipo de escenario de correo electrónico simulado que desea probar.

   - Si elige Custom (Personalizado) y aún está en el entorno aislado de Amazon SES, asegúrese de que la dirección en el campo Custom recipient (Destinatario personalizado) sea una dirección de correo electrónico verificada. Para obtener más información, consulte Creación de una identidad de dirección de correo electrónico.

7. Rellene los campos restantes como desee.
8. Elija Send Test Email (Enviar correo electrónico de prueba).
9. Inicie sesión en el cliente de correo electrónico de la dirección a la que ha enviado el correo electrónico. Encontrará el mensaje que ha enviado.

Uso del simulador de buzón de correo de forma manual

Amazon SES incluye un simulador de buzón de correo que puede utilizar para probar cómo su aplicación controla diferentes escenarios de envío de correo electrónico. El simulador de buzón de correo es útil cuando, por ejemplo, quiere probar una aplicación de envío de correo electrónico sin crear direcciones de correo electrónico ficticias, o cuando quiere encontrar el rendimiento máximo del sistema sin que se vea afectada su cuota de envío diaria.

Consideraciones importantes

Tenga en cuenta las siguientes características y limitaciones cuando utilice el simulador de buzón de correo de Amazon SES:

- Puede utilizar el simulador de buzón de correo aunque la cuenta esté en el entorno de pruebas de Amazon SES.
- Los correos electrónicos que envíe al proveedor de bandeja de correo están limitados por la velocidad de envío máxima de su cuenta, pero no afectan a sus cuotas de envío diario. Por ejemplo, si su cuenta está autorizada para enviar 10 000 mensajes por período de 24 horas y envía 100 mensajes al proveedor de bandeja de correo, todavía puede enviar hasta 10 000 mensajes a destinatarios habituales sin alcanzar su cuota de envío.
- Los correos electrónicos que envíe al simulador de bandeja de correo no afectan a las métricas de capacidad de entrega o de reputación de correo electrónico. Por ejemplo, si envía un gran número de mensajes a la dirección de rebote del simulador de correo electrónico, en la página de la consola de métricas de reputación no se muestra un mensaje advirtiéndole de que su tasa de rebotes es demasiado alta.
- A efectos de facturación, los mensajes de correo electrónico que envía al simulador de buzón de correo de Amazon SES son los mismos que cualquier otro correo electrónico que envía a través de Amazon SES. Es decir, le facturamos el mismo importe por los mensajes que envía al simulador de buzón de correo que por los que envía a destinatarios habituales.
- El simulador de bandeja de correo es compatible con el etiquetado, lo que le permite enviar correos electrónicos a la misma dirección del simulador de bandeja de correo de diversas maneras o para ver cómo la aplicación controla la ruta variable de retorno de sobres (VERP). Por ejemplo, puede enviar un correo electrónico a bounce+label1@simulator.amazonses.com y bounce +label2@simulator.amazonses.com para ver si su aplicación puede relacionar un mensaje rebotado con la dirección de correo electrónico que provocó el rebote.
- Si utiliza el simulador de buzón de correo para simular varios rebotes de la misma solicitud de envío, Amazon SES combina las respuestas de rebote en una sola.

Uso del simulador de buzón de correo

Para utilizar el simulador de correo electrónico, busque el escenario en la tabla siguiente y, a continuación, envíe un correo electrónico a la dirección de correo electrónico correspondiente.

> **Note**
>
> Cuando envíe un correo electrónico a una dirección del simulador de buzón de correo, debe hacerlo a través de Amazon SES mediante AWS CLI, un SDK de AWS, la consola de Amazon SES, la interfaz de SMTP de Amazon SES o la API de Amazon SES. El simulador de bandeja de correo no responde a los correos electrónicos que recibe de fuentes externas.

Escenario simulado	Email address
Entrega correcta: el proveedor de correo electrónico del destinatario acepta su correo electrónico. Si configuró las notificaciones de entrega como se describe en Configuración de las notificaciones de eventos para Amazon SES, Amazon SES le envía una notificación de entrega a través de Amazon Simple Notification Service (Amazon SNS).	success@simulator.amazonses.com
Rebote: el proveedor de correo electrónico del destinatario rechaza su correo electrónico con un código de respuesta SMTP 550 5.1.1 (“usuario desconocido”). Amazon SES genera una notificación de rebote y, en función de cómo haya configurado la cuenta, se la envía en un correo electrónico o envía una notificac ión a un tema de Amazon SNS. La dirección de correo electrónico del simulador de buzón de correo no se coloca en la lista de supresión de Amazon SES, lo que sucedería normalmen te al producirse un rechazo permanente. La respuesta de rebote que reciba desde el	bounce@simulator.amazonses.com

Escenario simulado	Email address
simulador de bandeja de correo cumple con RFC 3464. Para obtener más información acerca de cómo recibir retroalimentación de rebotes, consulte Configuración de las notificaciones de eventos para Amazon SES.	
Respuestas automáticas: el proveedor de correo electrónico del destinatario acepta su correo electrónico y lo envía a la bandeja de entrada del destinatario. El proveedor de correo electrónico envía una respuesta automática, como un mensaje de "fuera de la oficina" (OOTO), a la dirección que aparece en el encabezado Return-Path del correo electrónico, o a la dirección del remitente del sobre ("MAIL FROM") si no está presente el encabezado Return-Path. La respuesta automática que reciba desde el simulador de bandeja de correo cumple con RFC 3834.	ooto@simulator.amazonses.com

Escenario simulado	Email address
Reclamo: el proveedor de correo electrónico del destinatario acepta su correo electrónico y lo envía a la bandeja de entrada del destinatario. El destinatario decide que su mensaje no es solicitado y hace clic en “Mark as Spam” (Marcar como spam) en su cliente de correo electrónico. Amazon SES, a continuación, le reenvía la notificación de reclamo por correo electrónico o mediante una notificación de un tema de Amazon SNS, en función de cómo haya configurado la cuenta. La respuesta de reclamación que reciba desde el simulador de bandeja de correo cumple con RFC 5965. Para obtener más información acerca de cómo recibir retroalimentación de reclamaciones, consulte Configuración de las notificaciones de eventos para Amazon SES.	complaint@simulator.amazonses.com
Dirección del destinatario en la lista de supresión: Amazon SES genera un rechazo permanente como si la dirección del destinatario estuviera en la lista de supresión global.	suppressionlist@simulator.amazonses.com

Prueba de eventos de rechazo

Cada mensaje que envía a través de Amazon SES se analiza para detectar la presencia de virus. Si envía un mensaje que contiene un virus, Amazon SES acepta el mensaje, detecta el virus y rechaza el mensaje completo. Cuando Amazon SES rechaza el mensaje, deja de procesarlo y no intenta entregarlo al servidor de correo del destinatario. A continuación, genera un evento de rechazo.

El simulador de buzón de correo de Amazon SES no incluye una dirección para las pruebas de eventos de rechazo. Sin embargo, puede probar eventos de rechazo utilizando un archivo de prueba del Instituto Europeo para la Investigación de los Antivirus Informáticos (EICAR). Este archivo es un método estándar del sector para probar el software antivirus de una forma segura. Para crear un archivo de prueba EICAR, pegue el texto siguiente en un archivo:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Guarde el archivo como `sample.txt`, adjúntelo a un correo electrónico y, a continuación, envíe el correo electrónico a una dirección verificada. Si no hay ningún otro problema con el correo electrónico, Amazon SES acepta el mensaje, pero lo rechaza tal y como lo haría si tuviera un virus real.

> **Note**
>
> Los correos electrónicos rechazados, incluidos los que envía mediante el procedimiento anterior, se contabilizan para calcular su cuota de envío diaria. Le facturaremos cada mensaje que envíe, incluidos los rechazados.

Para obtener más información acerca de los archivos de prueba EICAR, consulte la página de archivo de prueba EICAR en Wikipedia.

Uso de conjuntos de configuración en Amazon SES

Los conjuntos de configuración son grupos de reglas que puede aplicar a sus identidades verificadas. Una identidad verificada es un dominio, un subdominio o una dirección de correo electrónico email que se utiliza para enviar correo electrónico a través de Amazon SES. Cuando aplica un conjunto de configuración a un correo electrónico, todas las reglas de dicho conjunto de configuración se aplican al correo electrónico.

Puede utilizar conjuntos de configuración para aplicar los siguientes tipos de reglas a su envío de correo electrónico, que pueden contener uno, ambos o ninguno de los tipos a continuación:

- Destinos de los eventos: te permiten publicar estadísticas de envío de correos electrónicos, como el número de envíos, entregas, aperturas, clics, rebotes y quejas sobre otros AWS productos por cada correo electrónico que envíes. Por ejemplo, puede enviar las métricas de su correo electrónico a un destino de Amazon Data Firehose y, a continuación, analizarlas con Amazon Managed Service para Apache Flink. Como alternativa, puede enviar información de rebotes y reclamos a Amazon SNS y recibir notificaciones de inmediato cuando se producen dichos eventos.
- Administración de grupos de IP: si alquila direcciones IP dedicadas para utilizarlas con Amazon SES, puede crear grupos de estas direcciones denominados grupos de IP dedicadas que podrá utilizar para enviar tipos específicos de correos electrónicos. Por ejemplo, puede asociar estos grupos de IP dedicadas a conjuntos de configuración y utilizar uno para el envío de comunicaciones de marketing y otro para el envío de correos electrónicos de transacciones. Su reputación de remitente para correos electrónicos de transacciones queda aislada de la de sus correos electrónicos de marketing.

Puede asociar un conjunto de configuración a una identidad verificada de las siguientes formas:

- Incluya una referencia al conjunto de configuración en los encabezados del correo electrónico. Para obtener más información acerca de la especificación de conjuntos de configuración en los mensajes de correo electrónico, consulte Especificar un conjunto de configuración al enviar correo electrónico.
- Especifique un conjunto de configuración existente que se utilizará como el conjunto de configuración predeterminada de identidad, ya sea en el momento de la creación de la identidad o posteriormente durante la edición de una identidad verificada. Consulte Comprensión de los conjuntos de configuración predeterminados.

Contenido

- Creación de conjuntos de configuración en SES
- Administración de conjuntos de configuración en Amazon SES
- Especificar un conjunto de configuración al enviar correo electrónico
- Visualización y exportación de métricas de reputación

Creación de conjuntos de configuración en SES

Puede utilizar la consola de SES, la acción `CreateConfigurationSet` en la API v2 de Amazon SES o el comando `aws sesv2 create-configuration-set` en la CLI v2 de Amazon SES para crear un nuevo conjunto de configuración. En esta sección, se muestra cómo crear conjuntos de configuración mediante la consola de SES y la CLI v2 de Amazon SES.

Creación de un conjunto de configuración (consola)

Para crear un conjunto de configuración utilizando la consola de SES, siga estos pasos:

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Configuration sets (Conjuntos de configuración).
3. Elija Create set (Crear conjunto).
4. Ingrese los siguientes detalles en la sección General details (Detalles generales):
    - Configuration set name (Nombre del conjunto de configuración): nombre del conjunto de configuración. El nombre puede contener un máximo de 64 caracteres alfanuméricos, incluyendo solamente letras, números, guiones (-) y guiones bajos (_).
    - Sending IP pool (Grupo de IP de envío): cuando envía correo electrónico utilizando este conjunto de configuración, los mensajes se envían desde las direcciones IP dedicadas del grupo asignado. Seleccione un grupo de IP de la lista.

> **Note**
>
> El (ses-default-dedicated-pool) default (predeterminado) contiene direcciones IP dedicadas que no se han asignado a ningún otro grupo. Para obtener más información acerca de la administración de grupos de IP, consulte Asignar grupos de IP.

- Opciones de seguimiento: seleccione la casilla de verificación Utilizar un dominio de redirección personalizado para utilizar un dominio de redirección personalizado para gestionar el seguimiento de clics y aperturas de este conjunto de configuración, en lugar de utilizar uno de los dominios de SES.
  - Custom redirect domain (Dominio de redirección personalizado): con un dominio de redirección personalizado, puede ingresar un subdominio personalizado en el cuadro (opcional) o bien seleccionar un dominio verificado de la lista.

> **Note**
>
> Los dominios de redirección personalizados se pueden especificar de la siguiente manera:
>
> - Los dominios de redirección deben configurarse antes de elegir esta opción. Para obtener instrucciones sobre cómo seleccionar un dominio personalizado para gestionar el seguimiento de aperturas y clics, consulte Configuración de dominios personalizados para gestionar seguimiento de mensajes abiertos y en los que se ha hecho clic.
> - A continuación, para elegir utilizar un dominio de redirección personalizado, debe indicarlo al crear el conjunto de configuración, o bien más adelante al editar las opciones de seguimiento para el conjunto de configuración.

- Advanced delivery options (Opciones de envío avanzadas): elija la flecha de la izquierda para expandir la sección de opciones de entrega avanzada.
  - Seguridad de la capa de transporte (TLS): para exigir que SES establezca una conexión segura con el servidor de correo de recepción y envíe correos electrónicos mediante el protocolo TLS, active la casilla Obligatorio.

> **Note**
>
> SES admite TLS 1.2 y recomienda TLS 1.3. Para obtener más información, consulte Seguridad de la infraestructura en SES.

5. Ingrese los siguientes detalles en la sección Reputation options (Opciones de reputación):

   - Métricas de reputación: se utilizan para rastrear las métricas de devoluciones y quejas de CloudWatch los correos electrónicos enviados con este conjunto de configuraciones. (Se aplican cargos adicionales; consulte el precio por métrica para ver CloudWatch.)
     - Enabled (Habilitado): active esta casilla para habilitar las métricas de reputación para el conjunto de configuración.

6. La sección Suppression list options (Opciones de lista de supresión) proporciona un conjunto de decisiones para definir la supresión personalizada, a partir de la opción de utilizar este conjunto de configuración para anular la supresión de nivel de cuenta. El mapa lógico de supresión de nivel de conjunto de configuración le ayudará a comprender los efectos de las combinaciones de anulación. Estas selecciones de anulaciones de varios niveles se pueden combinar para implementar tres niveles diferentes de supresión:

   a. Use account-level suppression (Utilizar supresión de nivel de cuenta): no anular la supresión de nivel de cuenta y no implementar ninguna supresión de nivel de conjunto de configuración; básicamente, cualquier correo electrónico enviado con este conjunto de configuración solo utilizará la supresión de nivel de cuenta. Para ello:

      - En Suppression list settings (Configuración de lista de supresión), desmarque la casilla Override account level settings (Anular la configuración de nivel de cuenta).

   b. Do not use any suppression (No utilizar ninguna supresión): anular la supresión de nivel de cuenta sin habilitar ninguna supresión de nivel de conjunto de configuración; esto significa que cualquier correo electrónico enviado con este conjunto de configuración no utilizará ninguna supresión de nivel de cuenta; en otras palabras, se cancelará toda supresión. Para ello:

      i. En Suppression list settings (Configuración de lista de supresión), marque la casilla Override account level settings (Anular la configuración de nivel de cuenta).

      ii. En Suppression list (Lista de supresión), desmarque la casilla Enabled (Habilitado).

c. Use configuration set-level suppression (Utilizar supresión de nivel de conjunto de configuración): anular la supresión de nivel de cuenta con configuraciones de la lista de supresión personalizada definida en este conjunto de configuración; esto significa que cualquier correo electrónico enviado con este conjunto de configuración solo utilizará su propia configuración de supresión e ignorará cualquier configuración de supresión de nivel de cuenta. Para ello:

   i. En Suppression list settings (Configuración de lista de supresión), marque la casilla Override account level settings (Anular la configuración de nivel de cuenta).

   ii. En Suppression list (Lista de supresión), marque Enabled (Habilitado).

   iii. En Specify the reason(s)... [Especificar el motivo (s)...], seleccione uno de los motivos de supresión que utilizará este conjunto de configuración.

7. En la sección de Virtual Deliverability Manager options (Opciones de Virtual Deliverability Manager) se le proporciona una forma de definir las configuraciones personalizadas sobre cómo este conjunto de configuración utilizará el seguimiento de las interacciones y la entrega compartida optimizada invalidando la forma en que se han definido en la configuración de Virtual Deliverability Manager al nivel de la cuenta:

   a. Para desactivar el seguimiento de las interacciones y la entrega compartida optimizada para este conjunto de configuración:

      i. Marque la casilla Override account level settings (Invalidar configuración a nivel de la cuenta).

      ii. Asegúrese de que la opción Enabled (Habilitado) no esté marcada para Engagement tracking (Seguimiento de las interacciones) y Optimized shared delivery (Entrega compartida optimizada) y, a continuación, elija Save changes (Guardar cambios).

   b. Para habilitar o desactivar o ambas el seguimiento de las interacciones y la entrega compartida optimizada para este conjunto de configuración:

      i. Marque la casilla Override account level settings (Invalidar configuración a nivel de la cuenta).

      ii. Marque o desmarque Enabled (Habilitado) para Engagement tracking (Seguimiento de las interacciones) y Optimized shared delivery (Entrega compartida optimizada) o para ambos y, a continuación, elija Save changes (Guardar cambios).

c. Para restablecer la configuración a nivel de la cuenta de Virtual Deliverability Manager sobre el seguimiento de las interacciones y la entrega compartida optimizada para este conjunto de configuración:

   - Desactive la casilla Override account level settings (Invalidar la configuración a nivel de la cuenta) y, a continuación, elija Save changes (Guardar cambios).

8. De manera opcional, puede agregar una o varias etiquetas en la sección Tags (Etiquetas). Repita los pasos siguientes para cada etiqueta que desee agregar al conjunto de configuración.

   a. Elija Add new tag (Agregar nueva etiqueta).
   b. Ingrese la Key (Clave) de la etiqueta.
   c. Ingrese el Value (Valor) de la etiqueta (opcional).

   Para eliminar una etiqueta que ha ingresado, elija Remove (Eliminar) para dicha etiqueta. Puede ingresar un máximo de 50 etiquetas.

9. Elija Create set (Crear conjunto) para crear su conjunto de configuración.

Ahora que ha creado el conjunto de configuración, tiene la opción de definir los destinos de eventos para el conjunto de configuración, lo que permite la publicación de eventos que se desencadena en los tipos de eventos que especifique para el destino del evento. Un conjunto de configuración puede tener varios destinos de eventos con varios tipos de eventos definidos. Consulte Crear destinos de eventos de Amazon SES.

Cree un conjunto de configuración (AWS CLI)

Puede crear un conjunto de configuración utilizando un archivo JSON como entrada para el comando `aws sesv2 create-configuration-set` en la AWS CLI.

1. Creación de un archivo JSON de entrada de la CLI

   Utilice su herramienta de edición de archivos favorita para crear un archivo JSON con las siguientes claves más los valores válidos para su entorno, o bien utilice el comando `aws sesv2 create-configuration-set` de la API v2 de SES con la opción `--generate-cli-skeleton` sin ningún valor especificado para imprimir una estructura JSON de ejemplo en la salida estándar.

   En este ejemplo, se utiliza un archivo con el nombre `create-configuration-set.json`:

```
{
    "ConfigurationSetName": "sample-configuration-set",
    "TrackingOptions": {
        "CustomRedirectDomain": "some.domain.com"
    },
    "DeliveryOptions": {
        "TlsPolicy": "REQUIRE",
        "SendingPoolName": "sending pool"
    },
    "ReputationOptions": {
        "ReputationMetricsEnabled": true,
        "LastFreshStart": timestamp
    },
    "SendingOptions": {
        "SendingEnabled": true
    },
    "Tags": [
        {
            "Key": "tag key",
            "Value": "tag value"
        }
    ],
    "SuppressionOptions": {
        "SuppressedReasons": ["BOUNCE","COMPLAINT"]
    }
}
```

> **Note**
>
> - Debe incluirla notación `file://` al principio de la ruta del archivo JSON.
> - La ruta del archivo JSON debe seguir la convención apropiada para el sistema operativo base donde se está ejecutando el comando. Por ejemplo, Windows utiliza la barra diagonal inversa (\) para hacer referencia a la ruta del directorio y Linux usa la barra diagonal (/).

2. Ejecute el siguiente comando utilizando el archivo que creó como entrada.

```
aws sesv2 create-configuration-set --cli-input-json file://create-configuration-set.json
```

> **Note**
>
> Para revisar la AWS CLI referencia de este comando, consulta create-configuration-set.

Administración de conjuntos de configuración en Amazon SES

Luego de crear un conjunto de configuración, puede administrarlo con las opciones ver, actualizar y eliminar mediante la consola de SES, la API v2 de Amazon SES y la CLI v2 de Amazon SES. Los conjuntos de configuración también se pueden asignar a una identidad verificada como conjunto de configuración predeterminado que se aplica cada vez que se envía un correo electrónico desde la identidad.

Temas de esta sección:

- Ver, editar y eliminar conjunto de configuración (consola)
- Conjuntos de configuración de lista (AWS CLI)
- Obtener los detalles del conjunto de configuración (AWS CLI)
- Eliminar un conjunto de configuración (AWS CLI)
- Detener el envío de correo electrónico desde un conjunto de configuración (AWS CLI)
- Comprensión de los conjuntos de configuración predeterminados
- Crear destinos de eventos de Amazon SES
- Asignación de grupos de IP en Amazon SES
- Configuración de dominios personalizados para gestionar seguimiento de mensajes abiertos y en los que se ha hecho clic

Ver, editar y eliminar conjunto de configuración (consola)

Acceder a la página de detalles de un conjunto de configuración existente

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Configuration sets (Conjuntos de configuración).
3. Para ver más detalles sobre un conjunto de configuración, elija Name (Nombre) de la lista de conjuntos de configuración. Esto le llevará a la página de detalles.

La página de detalles Configuration sets (Conjuntos de configuración) tiene dos pestañas para los detalles de conjuntos de configuración con paneles en cada pestaña donde podrá ver, editar o eliminar contenido de la siguiente manera:

- Pestaña Overview (Información general)
  - General details (Detalles generales): este panel muestra detalles generales para el conjunto de configuración:
    - Sending status (Estado de envío) (si está habilitado actualmente)
    - Configuration set name (Nombre del conjunto de configuración
    - Sending IP pool (Grupo de IP de envío)
    - Transport Layer Security (TLS)
    - Custom redirect domain (Dominio de redirección personalizado)
  - Reputation options (Opciones de reputación): este panel muestra detalles relacionados con su reputación de envío:
    - Reputation metrics (Métricas de reputación) (indica si está haciendo un seguimiento de las métricas)
    - Last fresh start (Último reinicio de) (fecha y hora en que se restablecieron por última vez las métricas de reputación del conjunto de configuración)
  - Suppression list options (Opciones de la lista de supresión): este panel muestra si va a invalidar la lista de supresión a nivel de la cuenta con la configuración establecida y, de ser así, cuáles son los detalles de la invalidación:
    - Suppression list settings (Configuración de la lista de supresión) (indica la invalidación de la configuración a nivel de la cuenta; de lo contrario, este es el único elemento que se muestra en el panel)
    - Suppression list (Lista de supresión) (indica cómo se invalida la configuración a nivel de la cuenta, ya sea con la lista de supresión habilitada o desactivada)
    - Suppression reasons (Motivos de supresión) (indica si las devoluciones o las quejas son el motivo por el que se agregan las direcciones de correo electrónico de los destinatarios a la lista de supresión)
  - Virtual Deliverability Manager options (Opciones de Virtual Deliverability Manager): este panel muestra si se va a invalidar la configuración de la cuenta de Virtual Deliverability Manager para el seguimiento de las interacciones y la entrega compartida optimizada con la configuración establecida y, de ser así, cuáles son los detalles de la invalidación:

    - Engagement tracking (Seguimiento de las interacciones) (indica si el seguimiento de las interacciones está habilitado o desactivado)
    - Optimized shared delivery (Entrega compartida optimizada) (indica si la entrega compartida optimizada está habilitada o desactivada)
- Etiquetas: este panel muestra todas las etiquetas que ha adjuntado al conjunto de configuración.
    - Clave
    - Valor

  Desde estos paneles, podrá realizar las acciones siguientes:

- Elija el icono Editar o, en el caso del panel Tags (Etiquetas), el botón Manage tags (Administrar etiquetas) para editar los detalles respectivos de cada panel.
- Para obtener más información acerca de los campos, consulte la sección relacionada en los pasos de Creación de un conjunto de configuración (consola).

> **Tip**
>
> Recuerde utilizar la opción Save changes (Guardar los cambios) cuando haya terminado la edición. Elija Cancel (Cancelar) para volver a la página de detalles del conjunto de configuración sin guardarla.

- Pestaña Event destinations (Destinos de eventos)
    - All destinations (***count of event destinations***) (Todos los destinos; recuento de destinos de eventos): este panel muestra todos los destinos de eventos que ha ingresado para su conjunto de configuración. Para cada destino, podrá ver lo siguiente:
        - Nombre
        - Destino
        - Event types (Tipos de eventos)
        - Event publishing (Publicación de eventos)

  Desde este panel, podrá realizar las acciones siguientes:

- Agregue un nuevo destino de evento al elegir el botón Add destination (Agregar destino). Para obtener más información acerca de la adición de destinos de evento, consulte Crear un destino de eventos.

- Modifique un destino de evento existente al seleccionar su nombre, que abrirá la pantalla de edición.
- Borre un destino de evento existente al marcar la casilla de verificación situada junto a su nombre y seleccionar el botón Delete (Borrar).

En la parte superior de la página de detalles de cada conjunto de configuración y visibles desde las pestañas Overview (Información general) o Events destination (Destino de eventos), encontrará las opciones siguientes:

- Delete (Eliminar): este botón eliminará su conjunto de configuración.
- Disable sending (Desactivar envío): este botón detendrá el envío de correos electrónicos desde su conjunto de configuración.

Conjuntos de configuración de lista (AWS CLI)

Puede usar el list-configuration-sets comando de AWS CLI para generar una lista de todos los conjuntos de configuraciones asociados a su cuenta en la región actual, de la siguiente manera:

```
aws sesv2 list-configuration-sets
```

Obtener los detalles del conjunto de configuración (AWS CLI)

Puede usar el get-configuration-set comando de AWS CLI para obtener detalles de un conjunto de configuraciones específico, de la siguiente manera:

```
aws sesv2 get-configuration-set --configuration-set-name name
```

Eliminar un conjunto de configuración (AWS CLI)

Puede utilizar el delete-configuration-set comando de AWS CLI para eliminar un conjunto de configuraciones específico, de la siguiente manera:

```
aws sesv2 delete-configuration-set --configuration-set-name name
```

Detener el envío de correo electrónico desde un conjunto de configuración (AWS CLI)

Puede usar el put-configuration-set-sending-options comando de AWS CLI para dejar de enviar correos electrónicos desde un conjunto de configuraciones específico, de la siguiente manera:

```
aws sesv2 put-configuration-set-sending-options --configuration-set-name name --no-sending-enabled
```

Para reanudar el envío, ejecute el mismo comando con la opción `--sending-enabled` en su lugar de la siguiente manera:

```
aws sesv2 put-configuration-set-sending-options --configuration-set-name name --sending-enabled
```

Comprensión de los conjuntos de configuración predeterminados

En esta sección se explica el concepto de asignar un conjunto de configuración como el conjunto predeterminado que usará una identidad verificada, para que pueda a comprender los beneficios y el caso de uso.

Un conjunto de configuración predeterminado aplica automáticamente sus reglas a todos los mensajes que envía desde la identidad de correo electrónico asociada a ese conjunto de configuración. Puede aplicar conjuntos de configuración predeterminados tanto a la dirección de correo electrónico como a las identidades de dominio durante la creación de la identidad o con posterioridad, como función de edición de una identidad existente.

Default configuration set considerations (Consideraciones de conjuntos de configuración predeterminados)

- El conjunto de configuración debe crearse primero antes de asociarlo a una identidad.
- Los conjuntos de configuración predeterminados solo se aplicarán si se verifica la identidad.
- Las identidades de correo electrónico solo se pueden asociar a un conjunto de configuración a la vez. Sin embargo, puede aplicar el mismo conjunto de configuración a varias identidades.
- Un conjunto de configuración predeterminado de nivel de dirección de correo electrónico anula un conjunto de configuración predeterminado de nivel de dominio. Por ejemplo, un conjunto de

configuración predeterminado asociado a joe@example.com anula el conjunto de configuración para el dominio de example.com.

- Un conjunto de configuración predeterminado a nivel de dominio se aplica a todas las direcciones de correo electrónico de ese dominio (a menos que verifique direcciones específicas para el dominio).
- Si elimina un conjunto de configuración designado como conjunto de configuración predeterminado para una identidad y, a continuación, intenta enviar correo electrónico a través de esa identidad, la llamada a Amazon SES falla y arroja un error de “solicitud incorrecta”.
- No se puede asignar un conjunto de configuración predeterminado a una identidad verificada que utilice un remitente delegado.
- Cómo especificar un conjunto de configuración existente que se utilizará como conjunto de configuración predeterminado de la identidad es en realidad una función de identidades verificadas, por lo que las instrucciones se incluyen en los flujos de trabajo de identidad:
  - Especificar un conjunto de configuración predeterminado durante la creación de identidades: siga las instrucciones que se indican en el paso 6 opcional para Conjunto de configuración predeterminada de identidad de dominio o Conjunto de configuración predeterminada de identidad de correo electrónico en el capítulo Creación y verificación de identidades en Amazon SES.
  - Especificar un conjunto de configuración predeterminado para una identidad existente: siga los pasos en Edición de una identidad mediante la consola junto con estos detalles para el paso 5:
    a. Elija la pestaña Configuration set (Conjunto de configuración).
    b. Elija Edit (Editar) en el contenedor Default configuration set (Conjunto de configuración predeterminada).
    c. Seleccione el cuadro de lista y elija un conjunto de configuración existente que se utilizará como predeterminado.
    d. Continúe con los pasos restantes en Edición de una identidad mediante la consola.

> **Note**
>
> Si el conjunto de configuración que asigne de forma predeterminada tiene habilitadas las métricas de reputación, se incurrirá en cargos adicionales por cualquier correo enviado con el conjunto de configuraciones predeterminado (consulte Precio por métrica para CloudWatch.

Crear destinos de eventos de Amazon SES

Los destinos de los eventos te permiten publicar las siguientes acciones de seguimiento del correo saliente en otros AWS servicios para su supervisión:

- Envíos
- Fallos de representación
- Rechazos
- Entregas
- Rebotes permanentes
- Reclamos
- Retrasos de entrega
- Suscripciones
- Aperturas
- Clics

Para obtener más información sobre la publicación de eventos, consulte the section called “Supervisar el envío de correo electrónico mediante la publicación de eventos”.

Crear un destino de eventos

Después de haber creado un conjunto de configuración, tiene la opción de crear los destinos de eventos para el conjunto de configuración, lo que permite la publicación de eventos que se desencadena en los tipos de eventos que especifique para el destino del evento. Un conjunto de configuración puede tener varios destinos de eventos con varios tipos de eventos definidos.

Si aún no ha creado ningún conjunto de configuración, consulte the section called “Creación de conjuntos de configuración”.

Los pasos siguientes muestran cómo crear o agregar un destino de eventos a un conjunto de configuración.

Para crear o agregar un destino de eventos mediante la consola de SES:

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.

2. En el panel de navegación, en Configuration (Configuración), elija Configuration sets (Conjuntos de configuración).
3. Elija un nombre del conjunto de configuración de la columna Name (Nombre) para acceder a sus detalles.
4. Seleccione la pestaña Event destinations (Destinos de eventos).
5. Elija Add destination.
6. Seleccione los tipos de evento.

   Los eventos de envío de correo electrónico son métricas relacionadas con su actividad de envío que puede medir mediante Amazon SES. En este paso, seleccione los tipos de eventos de envío de correo electrónico que desea que Amazon SES publique en su destino de evento.

   Para obtener más información acerca de los tipos de eventos, consulte Monitoreo de la actividad de envío de Amazon SES.

   a. Elija los Tipos de eventos que desea publicar.

      - Sending and delivery (Envío y entrega): para elegir los tipos de eventos que se van a publicar, active sus respectivas casillas de verificación, o bien elija Select all (Seleccionar todo) para publicar todos los tipos de eventos.

        Tipos de eventos

        - Sends (Envíos): la solicitud de envío se realizó en forma correcta y Amazon SES intentará entregar el mensaje al servidor de correo del destinatario.
        - Rendering Failures (Errores de representación): no se envió el correo electrónico debido a un problema con la presentación de la plantilla. Este tipo de evento se puede producir cuando faltan datos en la plantilla o cuando los parámetros y los datos de la plantilla no coinciden. (Este tipo de evento solo se produce cuando envía correo electrónico con las operaciones de la API `SendTemplatedEmail` o `SendBulkTemplatedEmail`).
        - Rejects (Rechazos): Amazon SES aceptó el correo electrónico, pero determinó que contenía un virus y no intentó entregarlo al servidor de correo del destinatario.
        - Deliveries (Entregas): Amazon SES entregó correctamente el correo electrónico al servidor de correo electrónico del destinatario.
        - Hard bounces (Rechazos permanentes): el servidor de correo del destinatario ha rechazado el correo electrónico de forma permanente. (Los rebotes temporales solo se

incluyen cuando Amazon SES no puede entregar el correo electrónico tras intentarlo durante un periodo de tiempo).

- Complaints (Reclamos): el correo electrónico se entregó correctamente al servidor de correo del destinatario, pero el destinatario lo marcó como spam.
- Delivery Delays (Retrasos de envío): el correo electrónico no se pudo entregar al servidor de correo del destinatario porque se produjo un problema temporal. Pueden producirse retrasos en la entrega, por ejemplo, si la bandeja de entrada del destinatario está llena o el servidor de recepción de email experimenta un problema transitorio. (Amazon Pinpoint no admite este tipo de evento).
- Subscriptions (Suscripciones): el correo electrónico se entregó correctamente, pero el destinatario actualizó las preferencias de suscripción haciendo clic en `List-Unsubscribe` en el encabezado del correo electrónico o el enlace `Unsubscribe` del pie de página. (Amazon Pinpoint no admite este tipo de evento).

- Open and clic tracking (Abrir y hacer clic): para medir el compromiso del suscriptor, active una o ambas casillas de verificación para realizar el seguimiento de aperturas y clics.
  - Opens (Aperturas): el destinatario recibió el mensaje y lo abrió en su cliente de correo electrónico.
  - Clicks (Clics): el destinatario hizo clic en uno o varios enlaces incluidos en el correo electrónico.

> **Note**
>
> La publicación de eventos de apertura y clic definida aquí, o en cualquier otro conjunto de configuraciones, no afecta a las opciones de seguimiento de las interacciones del panel de Virtual Deliverability Manager; estas se definen mediante la configuración de la cuenta de Virtual Deliverability Manager o las anulaciones del conjunto de configuración. Por ejemplo, si tiene desactivado el seguimiento de las interacciones a través de Virtual Deliverability Manager, no desactivará la publicación de eventos de apertura y clic que ha configurado aquí en los destinos de eventos de SES.

  - Configuration set redirect domain (Dominio de redireccionamiento de conjunto de configuración): este campo aparecerá y se rellenará previamente con el nombre del dominio de redireccionamiento personalizado si ha asignado uno al crear el conjunto de configuración.

> **Note**
>
> Puede actualizar el Custom redirect domain (Dominio de redirección personalizado) en el conjunto de configuración para realizar el seguimiento de aperturas y clics en ese dominio. Consulte Tracking options (Opciones de seguimiento) en el paso 4 de Creación de conjuntos de configuración. Para obtener más información acerca de la configuración de dominios de aperturas y clics personalizados, consulte Configuración de dominios personalizados para gestionar seguimiento de mensajes abiertos y en los que se ha hecho clic.

b. Elija Siguiente para continuar.

7. Especifique el destino.

   El destino de un evento es un AWS servicio en el que se pueden publicar eventos de envío de correo electrónico. Elegir el destino adecuado depende del nivel de detalle que desee capturar y cómo desea recibir los datos.

   a. Opciones de destino

   - Tipo de destino: al seleccionar el botón de radio situado junto al AWS servicio en el que publicar los eventos, aparecerá un panel de detalles con los campos correspondientes al servicio. Al seleccionar los enlaces a continuación se darán instrucciones acerca del panel de detalles del servicio:
     - Amazon CloudWatch (se aplican cargos adicionales; consulte el precio por métrica para ver) CloudWatch.
     - Amazon Data Firehose
     - Amazon EventBridge
     - Amazon Pinpoint (No admite los tipos de eventos Delivery delays [Retrasos de entrega] ni Subscriptions [Suscripciones]).
     - Amazon SNS

     Para obtener más información acerca de cómo utilizar el modelo de publicación de eventos para monitorear la operación de correo electrónico, consulte Monitoreo del envío de correo electrónico mediante la publicación de eventos de Amazon SES.
   - Name (Nombre): ingrese el nombre del destino de este conjunto de configuración. El nombre solo puede contener letras, números y guiones.

- Event publishing (Publicación de eventos): para activar la publicación de eventos para este destino, active la casilla de verificación Enabled (Habilitado).

b. Elija Siguiente para continuar.

8. Revisión

   Cuando haya comprobado que las entradas son correctas, elija Add destination (Agregar destino) para agregar su destino de eventos.

También puede crear un destino de eventos mediante la consola de Amazon SES, la API v2 de Amazon SES o la CLI v2 de Amazon SES.

Para crear un destino de eventos mediante la API SES:

- Para la creación de un destino de eventos mediante la API SES, consulte `CreateConfigurationSetEventDestination`.

Editar, desactivar, habilitar o eliminar un destino de eventos

Siga estos pasos para editar, desactivar, habilitar o eliminar un destino de eventos mediante la consola de SES:

Para editar, desactivar, habilitar o eliminar un destino de eventos mediante la consola de SES:

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Configuration sets (Conjuntos de configuración).
3. Elija un nombre del conjunto de configuración de la columna Name (Nombre) para acceder a sus detalles.
4. Seleccione la pestaña Event destinations (Destinos de eventos) del conjunto de configuración.
5. Seleccione el nombre del destino del evento en la columna Name (Nombre).
6.
   - Para editar: elija el botón Edit (Editar) en el panel correspondiente para el conjunto de campos que desea editar y realice los cambios seguidos de Save changes (Guardar cambios).
   - Para desactivar o habilitar: elija el botón etiquetado Disable (Desactivar) o Enable (Habilitar) en la esquina superior derecha.
   - Para eliminar: elija el botón Delete (Eliminar) de la esquina superior derecha.

También puede editar, desactivar, habilitar o eliminar un destino de eventos mediante la consola de Amazon SES, la API v2 de Amazon SES o la CLI v2 de Amazon SES.

Para editar, desactivar, habilitar o eliminar un destino de eventos mediante la API de SES:

1. Para desactivar o habilitar un destino de eventos mediante la API de SES, consulte `UpdateConfigurationSetEventDestination`.
2. Para eliminar un destino de eventos mediante la API de SES, consulte `DeleteConfigurationSetEventDestination`.

Asignación de grupos de IP en Amazon SES

Puede utilizar grupos de IP para crear grupos de direcciones IP dedicadas para enviar determinados tipos de correo electrónico. También puede utilizar un grupo de direcciones IP que compartan todos los clientes de Amazon SES.

Al asignar un grupo de IP a un conjunto de configuración, puede elegir entre las opciones siguientes:

- Un grupo de IP dedicado específico: al seleccionar un conjunto de IP dedicado existente, los correos electrónicos que utilizan el conjunto de configuración se utilizan solo las direcciones IP dedicadas que perteneces a dicho grupo. Para conocer los procedimientos sobre cómo crear:
  - nuevos grupos de IP estándar, consulte Creación de grupos de IP dedicadas estándar para IP dedicadas (estándar).
  - nuevos grupos de IP administradas, consulte Creación de un grupo de IP administradas para habilitar IP dedicadas (administradas).
- ses-default-dedicated-pool: este grupo contiene todas las direcciones IP dedicadas para su cuenta que no pertenecen ya a un grupo de IP. Si envía un correo electrónico utilizando un conjunto de configuración que no está asociado a un grupo, o si envía un correo electrónico sin especificar ningún conjunto de configuración, el correo electrónico se envía desde una de las direcciones de este grupo predeterminado. SES administra automáticamente este grupo y no puede editarse.
- ses-shared-pool: este grupo contiene un conjunto grande de direcciones IP compartidas entre todos los clientes de Amazon SES. Esta opción puede resultar útil cuando necesita enviar correo electrónico que no se ajusta a sus comportamientos de envío habituales.

Asignación de un grupo de IP a un conjunto de configuración

En esta sección se hace referencia a los procedimientos que deben seguirse para asignar y modificar grupos de IP en un conjunto de configuración mediante la consola de Amazon SES.

- Para asignar un grupo de IP a un conjunto de configuración mediante la consola…
  - Mientras crea un nuevo conjunto de configuración: consulte Grupo de IP de envío en el Paso 4 de Creación de conjuntos de configuración.
  - mientras modifica un conjunto de configuración existente: seleccione el botón Edit (Editar) en el panel General details (Detalles generales) del conjunto de configuración seleccionado y siga las instrucciones de Grupo de IP de envío, en el paso 4 de Creación de conjuntos de configuración.

Configuración de dominios personalizados para gestionar seguimiento de mensajes abiertos y en los que se ha hecho clic

Cuando se utiliza la publicación de eventos para capturar los eventos de mensajes abiertos y en los que se ha hecho clic, Amazon SES realiza pequeños cambios en los emails que se envían. Para capturar eventos abiertos, SES agrega una imagen GIF transparente de 1 píxel por 1 píxel en cada correo electrónico enviado a través de SES, que incluye un nombre de archivo único para cada correo electrónico y se aloja en un servidor operado por SES; cuando se descarga la imagen, SES puede indicar exactamente qué mensaje se abrió y quién lo ha abierto.

De forma predeterminada, este píxel se inserta en la parte inferior del correo electrónico; sin embargo, algunas aplicaciones de proveedores de correo electrónico truncan la vista previa de un correo electrónico cuando supera un determinado tamaño y pueden proporcionar un enlace para ver el resto del mensaje. En este escenario, la imagen de seguimiento de píxeles de SES no se carga y eliminará las tasas de apertura que intenta rastrear. Para evitar esto, puede colocar de forma opcional el píxel al principio del correo electrónico o en cualquier otro lugar mediante la inserción del marcador de posición `{{ses:openTracker}}` en el cuerpo del correo electrónico. Una vez que SES recibe el mensaje con el marcador de posición, se sustituirá por una imagen de píxel de seguimiento abierta.

> **Important**
>
> Simplemente agregue un marcador de posición `{{ses:openTracker}}`, ya que más de uno provocará que se devuelva un código de error `400 BadRequestException`.

Para capturar los eventos de clics de enlaces, Amazon SES reemplaza los enlaces de los correos electrónicos por enlaces a un servidor operado por SES. Esto redirige inmediatamente al destinatario a su destino previsto.

También tiene la opción de utilizar sus propios dominios, en lugar de los dominios que posee y opera Amazon SES, con el objetivo de crear una experiencia más coherente para los destinatarios, lo que significa que se eliminan todos los indicadores de SES. Puede configurar varios dominios personalizados para gestionar eventos de seguimiento de mensajes abiertos y en los que se ha hecho clic. Estos dominios personalizados están asociados a conjuntos de configuración. Cuando envíe un correo electrónico a través de un conjunto de configuración, si dicho conjunto de configuración está configurado para utilizar un dominio personalizado, entonces los enlaces de clic y mensaje abierto en dicho correo electrónico utilizan automáticamente el dominio personalizado especificado en dicho conjunto de configuración.

Esta sección contiene procedimientos para configurar un subdominio en un servidor de su propiedad destinado a redirigir automáticamente a los usuarios a los servidores de seguimiento de mensajes abiertos y en los que se ha hecho clic operados por Amazon SES. Hay tres pasos implicados en la configuración de estos dominios. En primer lugar, debe configurar el propio subdominio, a continuación, un conjunto de configuración para utilizar el dominio personalizado y, por último, configure su destino de eventos para publicar eventos de apertura y de clic. Este tema contiene procedimientos para completar todos estos pasos.

Sin embargo, si simplemente desea habilitar el seguimiento de apertura o clic sin configurar un dominio personalizado, puede proceder directamente a definir los destinos de eventos para el conjunto de configuración, lo que permite la publicación de eventos que se desencadena en los tipos de eventos que especifique, incluidos los eventos de apertura y clic. Un conjunto de configuración puede tener varios destinos de eventos con varios tipos de eventos definidos. Consulte Crear destinos de eventos de Amazon SES.

Parte 1: Configurar un dominio para gestionar redirecciones de seguimiento de mensajes abiertos y en los que se ha hecho clic

Los procedimientos específicos para configurar un dominio de redireccionamiento varían en función de su proveedor de servicios de alojamiento web (y su red de entrega de contenido, si utiliza un servidor HTTPS). Los procedimientos de las secciones siguientes ofrecen directrices generales en lugar de pasos específicos.

Opción 1: configuración de un dominio HTTP

Si planea utilizar un dominio HTTP para gestionar mensajes abiertos y en los que se ha hecho clic (en contraposición a un dominio HTTPS), el proceso para configurar el subdominio conlleva únicamente algunos pasos.

> **Note**
>
> Si configura un dominio personalizado que utilice el protocolo HTTP y envía un correo electrónico que contiene vínculos que utilizan el protocolo HTTPS, los clientes podrían ver un mensaje de advertencia cuando hacen clic en los enlaces de su correo electrónico. Si tiene previsto enviar correos electrónicos que contengan enlaces que utilicen el protocolo HTTPS, debería utilizar un dominio HTTPS para gestionar los eventos de seguimiento en los que se ha hecho clic.

Para configurar un subdominio HTTP para la gestión del seguimiento de mensajes abiertos y en los que se ha hecho clic

1. Si aún no lo ha hecho, cree un subdominio que utilizar para enlaces de seguimiento de mensajes abiertos y en los que se ha hecho clic. Le recomendamos que cree un subdominio dedicado específicamente a la gestión de estos enlaces.
2. Compruebe el subdominio para utilizarlo con Amazon SES. Para obtener más información, consulte Creación de una identidad de dominio.
3. Modifique el registro de DNS del subdominio. En el registro de DNS, agregue un nuevo registro CNAME que redirija las solicitudes al dominio de seguimiento de Amazon SES. La dirección a la que se redirige depende de la AWS región en la que utilice Amazon SES. La siguiente tabla contiene una lista de dominios de seguimiento para las regiones de AWS donde Amazon SES está disponible.

AWS Región	AWS dominio de seguimiento
US East (Ohio)	`r.us-east-2.awstrack.me`
Este de EE. UU. (Norte de Virginia)	`r.us-east-1.awstrack.me`
Oeste de EE. UU. (Norte de California)	`r.us-west-1.awstrack.me`

AWS Región	AWS dominio de seguimiento
Oeste de EE. UU. (Oregón)	`r.us-west-2.awstrack.me`
África (Ciudad del Cabo)	`r.af-south-1.awstrack.me`
Asia-Pacífico (Yakarta)	`r.ap-southeast-3.awstrack.me`
Asia-Pacífico (Bombay)	`r.ap-south-1.awstrack.me`
Asia-Pacífico (Osaka)	`r.ap-northeast-3.awstrack.me`
Asia-Pacífico (Seúl)	`r.ap-northeast-2.awstrack.me`
Asia-Pacífico (Singapur)	`r.ap-southeast-1.awstrack.me`
Asia-Pacífico (Sídney)	`r.ap-southeast-2.awstrack.me`
Asia-Pacífico (Yakarta)	r.ap-southeast-3.awstrack.me
Asia-Pacífico (Yakarta)	r.ap-southeast-3.awstrack.me
Asia-Pacífico (Tokio)	`r.ap-northeast-1.awstrack.me`
Canadá (centro)	`r.ca-central-1.awstrack.me`
Europa (Fráncfort)	`r.eu-central-1.awstrack.me`
Europa (Irlanda)	`r.eu-west-1.awstrack.me`
Europa (Londres)	`r.eu-west-2.awstrack.me`
Europa (Milán)	`r.eu-south-1.awstrack.me`
Europa (Estocolmo)	`r.eu-north-1.awstrack.me`
Israel (Tel Aviv)	`r.il-central-1.awstrack.me`
Medio Oriente (Baréin)	`r.me-south-1.awstrack.me`
América del Sur (São Paulo)	`r.sa-east-1.awstrack.me`

AWS Región	AWS dominio de seguimiento
AWS GovCloud (US-Oeste)	`r.us-gov-west-1.awstrack.me`
AWS GovCloud (EEUU-Este)	`r.us-gov-east-1.awstrack.me`

> **Note**
>
> En función de su proveedor de servicios de alojamiento web, puede tardar varios minutos en que los cambios que haga en el registro de DNS del subdominio surtan efecto. Su proveedor de servicios de alojamiento web u organización de TI puede proporcionarle información adicional acerca de estos retrasos.

Opción 2: configuración de un dominio HTTPS

También puede utilizar un dominio HTTPS para realizar un seguimiento de los clics en los enlaces. Para configurar un dominio HTTPS para realizar un seguimiento de los clics de enlaces, debe realizar algunos pasos adicionales, además de los necesarios para setting up an HTTP domain (configurar un dominio HTTP).

> **Note**
>
> También puede utilizar un dominio HTTPS para realizar un seguimiento de los clics en los enlaces. Amazon SES solo admite el seguimiento abierto sobre dominios HTTP cuando se utiliza un dominio personalizado; de lo contrario, SES admite el seguimiento abierto sobre HTTPS cuando no se define un dominio personalizado, que utilizará implícitamente los dominios propiedad de SES y operados por SES.

Para configurar un subdominio HTTPS para la gestión de enlaces de clic

1. Crear un subdominio que desea utilizar para enlaces de mensajes en los que se ha hecho clic. Le recomendamos que cree un subdominio dedicado específicamente a la gestión de estos enlaces.
2. Compruebe el subdominio para utilizarlo con Amazon SES. Para obtener más información, consulte Creación de una identidad de dominio.

3. Cree una cuenta nueva en una red de entrega de contenido (CDN), como Amazon CloudFront.
4. Configure la CDN en el origen, que es el dominio de seguimiento de SES, como por ejemplo `r.us-east-1.awstrack.me`. La CDN debe pasar el encabezado `Host` proporcionado por el solicitante al origen. Consulte este artículo de AWS re:Post para obtener más información. La dirección que utilice dependerá de la Región de AWS que utilice en SES. La siguiente tabla contiene una lista de los dominios de seguimiento de las AWS regiones en las que SES está disponible.

AWS Región	AWS dominio de seguimiento
US East (Ohio)	`r.us-east-2.awstrack.me`
Este de EE. UU. (Norte de Virginia)	`r.us-east-1.awstrack.me`
Oeste de EE. UU. (Norte de California)	`r.us-west-1.awstrack.me`
Oeste de EE. UU. (Oregón)	`r.us-west-2.awstrack.me`
África (Ciudad del Cabo)	`r.af-south-1.awstrack.me`
Asia-Pacífico (Yakarta)	`r.ap-southeast-3.awstrack.me`
Asia-Pacífico (Bombay)	`r.ap-south-1.awstrack.me`
Asia-Pacífico (Osaka)	`r.ap-northeast-3.awstrack.me`
Asia-Pacífico (Seúl)	`r.ap-northeast-2.awstrack.me`
Asia-Pacífico (Singapur)	`r.ap-southeast-1.awstrack.me`
Asia-Pacífico (Sídney)	`r.ap-southeast-2.awstrack.me`
Asia-Pacífico (Tokio)	`r.ap-northeast-1.awstrack.me`
Canadá (centro)	`r.ca-central-1.awstrack.me`
Europa (Fráncfort)	`r.eu-central-1.awstrack.me`
Europa (Irlanda)	`r.eu-west-1.awstrack.me`

AWS Región	AWS dominio de seguimiento
Europa (Londres)	`r.eu-west-2.awstrack.me`
Europa (Milán)	`r.eu-south-1.awstrack.me`
Europa (Estocolmo)	`r.eu-north-1.awstrack.me`
Israel (Tel Aviv)	`r.il-central-1.awstrack.me`
Medio Oriente (Baréin)	`r.me-south-1.awstrack.me`
América del Sur (São Paulo)	`r.sa-east-1.awstrack.me`
AWS GovCloud (EE. UU.-Oeste)	`r.us-gov-west-1.awstrack.me`
AWS GovCloud (EEUU-Este)	`r.us-gov-east-1.awstrack.me`

5. Si usa Route 53 para administrar la configuración de DNS de su dominio y CloudFront como CDN, cree un registro de alias en Route 53 que haga referencia a su CloudFront distribución (por ejemplo, d111111abcdef8.cloudfront.net). Para obtener más información, consulte Creación de registros con la consola de Amazon Route 53 en la Guía para desarrolladores de Amazon Route 53.

   De lo contrario, en la configuración de DNS de su subdominio, añada un registro CNAME que haga referencia a la dirección de su CDN.

6. Adquiera un certificado SSL a partir de una autoridad de certificación de confianza. El certificado debería cubrir tanto el subdominio que creó en el paso 1, así como la CDN que ha configurado en los pasos 3 a 5. Cargue el certificado en la CDN.

Parte 2: Configurar un conjunto de configuración para hacer referencia a un dominio de seguimiento de mensajes abiertos y en los que se ha hecho clic personalizado

Después de configurar su dominio para gestionar redirecciones de seguimiento de mensajes abiertos y en los que se ha hecho clic, debe especificar su dominio personalizado en el conjunto de configuración. Puede completar este paso mediante la consola de Amazon SES o la operación de la API `CreateConfigurationSetTrackingOptions`.

En esta sección se hace referencia a los procedimientos que debe seguir para completar estas tareas mediante la consola de Amazon SES. Para obtener información sobre el uso de la API, consulte CreateConfigurationSetTrackingOpciones en la referencia de la API de Amazon Simple Email Service.

- Para especificar un dominio de redireccionamiento personalizado mediante la consola...
  - Mientras crea un nuevo conjunto de configuración: consulte Opciones de seguimiento en el Paso 4 de Creación de conjuntos de configuración.
  - mientras modifica un conjunto de configuración existente: seleccione el botón Edit (Editar) en el panel General details (Detalles generales) del conjunto de configuración seleccionado y siga las instrucciones que se describen en Opciones de seguimiento, en el paso 4 de Creación de conjuntos de configuración.

Parte 3: Selección de tipos de eventos de apertura y clic en los destinos de eventos del conjunto de configuración

Después de especificar el dominio personalizado en el conjunto de configuración, debe seleccionar tipos de eventos abiertos o hacer clic en un destino de eventos agregado al conjunto de configuración. Puede completar este paso mediante la consola de Amazon SES o la operación de la API `CreateConfigurationSetEventDestination`.

- Para seleccionar tipos de eventos abiertos o clic mediante la consola...
  - al crear un nuevo destino de evento, consulte Seguimiento de abrir y clic en el paso 6 de the section called “Crear un destino de eventos”.
  - al modificar un destino de evento existente, seleccione el botón Edit (Editar) en el panel Event types (Tipos de evento) del destino de eventos seleccionado en el paso 6 de the section called “Editar, desactivar, habilitar o eliminar un destino de eventos”

Especificar un conjunto de configuración al enviar correo electrónico

Para utilizar un conjunto de configuración al enviar un correo electrónico, debe transferir el nombre del mismo de los encabezados del correo electrónico. Todos los métodos de envío de correo electrónico de Amazon SES, como la AWS CLI, los AWS SDK y la interfaz SMTP de Amazon SES,

le permiten transferir un conjunto de configuraciones en los encabezados del correo electrónico que envíe.

Si utiliza la interfaz de SMTP o la operación de la API `SendRawEmail`, puede especificar un conjunto de configuración incluyendo el siguiente encabezado en su correo electrónico (sustituyendo *`ConfigSet`* por el nombre del conjunto de configuración que desee utilizar):

```
X-SES-CONFIGURATION-SET: ConfigSet
```

En esta guía se incluyen ejemplos de código para enviar correo electrónico con los AWS SDK y la interfaz de SMTP de Amazon SES. Cada uno de estos ejemplos incluye un método para especificar un conjunto de configuración. Para ver step-by-step los procedimientos de envío de correos electrónicos que incluyen referencias a los conjuntos de configuración, consulte lo siguiente:

- Envío de correo electrónico a través de Amazon SES mediante un AWS SDK
- Uso de la interfaz de SMTP de Amazon SES para enviar correo electrónico

Visualización y exportación de métricas de reputación

Amazon SES exporta automáticamente a Amazon CloudWatch la información sobre las tasas generales de devoluciones y reclamaciones de toda tu cuenta. Puede usar estas métricas para crear alarmas o pausar automáticamente el envío de correos electrónicos mediante una función Lambda. CloudWatch

También puede exportar las métricas de reputación de conjuntos de configuraciones individuales a CloudWatch. La exportación de los datos de reputación en el nivel de conjunto de configuración le ofrece mayor control sobre su reputación como remitente.

En esta sección se incluyen los procedimientos para exportar los datos de reputación de conjuntos de configuraciones individuales CloudWatch mediante la API de Amazon SES.

Habilitación de la exportación de métricas de reputación

Para comenzar a exportar las métricas de reputación de un conjunto de configuración, use la operación de la API `UpdateConfigurationSetReputationMetricsEnabled`. Para acceder a la API de Amazon SES, le recomendamos que utilice el AWS CLI o uno de los AWS SDK.

En este procedimiento se presupone que AWS CLI está instalado en su ordenador y que está configurado correctamente. Para obtener más información sobre la instalación y configuración del AWS CLI, consulte la Guía del AWS Command Line Interface usuario.

Para habilitar la exportación de métricas de reputación de un conjunto de configuración

- En la línea de comando, escriba el comando siguiente:

```
aws ses update-configuration-set-reputation-metrics-enabled --configuration-set-
name ConfigSet --enabled
```

  Sustituya *ConfigSet*el comando anterior por el nombre del conjunto de configuraciones para el que quiere empezar a exportar las métricas de reputación.

Desactivación de la exportación de métricas de reputación

También puede usar la operación de la API `UpdateConfigurationSetReputationMetricsEnabled` para deshabilitar la exportación de métricas de reputación de un conjunto de configuración.

Para deshabilitar la exportación de métricas de reputación de un conjunto de configuración

- En la línea de comando, escriba el comando siguiente:

```
aws ses update-configuration-set-reputation-metrics-enabled --configuration-set-
name ConfigSet --no-enabled
```

  Sustituya *ConfigSet*el comando anterior por el nombre del conjunto de configuraciones para el que desea deshabilitar la exportación de métricas de reputación.

Direcciones IP dedicadas para Amazon SES

Al crear una nueva cuenta de Amazon SES, de forma predeterminada, sus correos electrónicos se envían desde direcciones IP que se comparten con otros usuarios de SES. También puede utilizar direcciones IP dedicadas que están reservadas para su uso exclusivo alquilándolas por un coste adicional. Esto le da un control total sobre la reputación de su remitente y le permite aislar su reputación para diferentes segmentos en los programas de correo electrónico. Amazon SES ofrece dos formas de aprovisionar y administrar una dirección IP dedicada:

- Estándar: se refiere a las direcciones IP dedicadas que se configuran y administran manualmente, lo que incluye la opción de prepararlas y escalarlas manualmente, y de moverlas manualmente dentro y fuera de los grupos de IP. (Anteriormente, se las denominaba direcciones IP dedicadas en SES).
- Administradas: se refiere a las direcciones IP dedicadas que SES configura automáticamente en su nombre para proporcionar una forma rápida y sencilla de empezar a utilizar direcciones IP dedicadas administradas por SES. Se preparan automáticamente para cada ISP de forma individual y se escalan automáticamente según el volumen de envíos para ayudar a garantizar que sus direcciones IP dedicadas se utilicen de la manera óptima en función de la forma en que envíe el correo electrónico.

Cuando tenga decidir entre las direcciones IP compartidas o los dos tipos de direcciones IP dedicadas que se han definido antes, elija las que tengan más beneficios para el tipo, el volumen y los patrones de correo electrónico que envía. Para ayudarle a tomar su decisión, estos beneficios se resumen en la tabla siguiente. Elija un elemento de la columna Beneficio para obtener información adicional.

Beneficio	Direcciones IP compartidas	Direcciones IP dedicadas (estándar)	Direcciones IP dedicadas (administradas)
Se pueden utilizar de inmediato	Sí	No	No
Se requiere una configuración adicional	No	Sí	Sí

Beneficio	Direcciones IP compartidas	Direcciones IP dedicadas (estándar)	Direcciones IP dedicadas (administradas)
Direcciones IP y reputación aisladas de otros clientes de SES	No	Sí	Sí
La capacidad aumenta automáticamente a medida que aumenta el tráfico	No	No	Sí
Bueno para clientes con patrones de envío continuos y predecibles	Sí	Sí	Sí
Bueno para clientes con patrones de envío menos predecibles	Sí	No	Sí
Bueno para remitentes de gran volumen	Sí	Sí	Sí
Bueno para remitentes de bajo volumen	Sí	No	No
Costos mensuales adicionales	No	Sí	Sí
Control completo sobre la reputación del remitente	No	Sí	Sí

Beneficio	Direcciones IP compartidas	Direcciones IP dedicadas (estándar)	Direcciones IP dedicadas (administradas)
Aislar reputación por correo electrónico tipo, destinatario u otros factores	No	Sí	Sí
Ofrece direcciones IP conocidas que no cambian nunca	No	Sí	No

> **Important**
>
> Si no tiene previsto enviar grandes volúmenes de correo electrónico de forma regular y predecible, le recomendamos que utilice direcciones IP compartidas. Si desea utilizar direcciones IP dedicadas en situaciones en las que los patrones de envío son muy irregulares, el uso de IP dedicadas (administradas) es la mejor opción.

Facilidad de configuración

Direcciones IP compartidas: no es necesario realizar ninguna configuración adicional. Su cuenta de SES está lista para enviar correo electrónico en cuanto verifique una dirección de correo electrónico y salga del entorno aislado.

Direcciones IP dedicadas (estándar): debe enviar una solicitud a través del AWS Support Center y, si lo desea, configurar grupos de IP dedicadas.

Direcciones IP dedicadas (administradas): no es necesario que envíe una solicitud para las direcciones IP dedicadas. Se asignan automáticamente cuando se inscribe y realizan un recorrido único para crear su grupo dedicado administrado.

Administración de la reputación

La reputación de las direcciones IP se basa en gran medida en los patrones de envío históricos y en el volumen. Una dirección IP que envía volúmenes coherentes de correo electrónico durante un largo periodo de tiempo, normalmente tiene una buena reputación.

Direcciones IP compartidas: se comparten entre varios clientes de SES. Estas direcciones envían de forma colectiva un gran volumen de correo electrónico y AWS administra cuidadosamente el tráfico saliente para maximizar la reputación de las direcciones IP compartidas.

Direcciones IP dedicadas (estándar): tras el calentamiento, sus direcciones IP se aíslan del conjunto compartido de SES y usted mantiene su propia reputación como remitente mediante el envío de volúmenes de correo electrónico consistentes y predecibles.

Direcciones IP dedicadas (administradas): tras el calentamiento de las nuevas IP, se aíslan del conjunto compartido de SES y usted conserva su propia reputación de remitente. La ventaja adicional es hacer un seguimiento de la reputación de cada ISP y programar de forma óptima los envíos salientes en consecuencia. Por lo tanto, mientras mantiene su reputación de remitente, esta automatización ayuda a mejorar la capacidad de entrega general y a reducir las tasas de devoluciones en comparación con las cargas de trabajo equivalentes en direcciones IP dedicadas configuradas manualmente.

> **Note**
>
> Para obtener información acerca de los datos de Smart Network Data Services (SNDS) para sus IP dedicadas, consulte Métricas de SNDS para direcciones IP dedicadas.

Capacidad de predicción de los patrones de envío

Una dirección IP con un historial de envío de correo electrónico coherente tiene una mejor reputación que otra que de repente comienza a enviar grandes volúmenes de correo electrónico sin un historial previo de envíos.

Direcciones IP compartidas: son adecuadas para patrones de envío de correo electrónico que no siguen un patrón predecible. Con las direcciones IP compartidas, puede aumentar o reducir sus patrones de envío de correo electrónico en función de las demandas de la situación.

Direcciones IP dedicadas (estándar): debe preparar las direcciones enviando una cantidad de correo electrónico que aumenta gradualmente cada día. El proceso de preparación de nuevas direcciones IP se describe en Preparación de direcciones IP dedicadas (estándar). Una vez que las direcciones IP dedicadas estén preparadas, debe mantener un patrón de envío coherente.

Direcciones IP dedicadas (gestionadas): sus direcciones IP dedicadas se calientan automáticamente para cada IP del grupo gestionado mediante una estrategia de calentamiento adaptable (en combinación con el grupo compartido de SES) que tiene en cuenta los patrones de envío reales para optimizar el calentamiento para cada ISP de forma individual. El conjunto de direcciones IP gestionadas se amplía automáticamente por ISP en función del uso y de la consideración de las políticas específicas del ISP.

Volumen de correo electrónico saliente

Direcciones IP compartidas: son ideales para los clientes que envían poco volumen de correo electrónico.

Direcciones IP dedicadas (estándar) | Direcciones IP dedicadas (administradas): ambas son adecuadas para clientes que envían grandes volúmenes de correo electrónico. La mayoría de los ISP solo realizan un seguimiento de la reputación de una determinada dirección IP si reciben un volumen importante de correo desde esa dirección. Para cada ISP con el que desee cultivar una reputación, debe enviar varios cientos de mensajes de correo electrónico en un periodo de 24 horas, al menos una vez al mes. En algunos casos, ambos tipos de direcciones IP dedicadas también pueden funcionar para volúmenes de correo electrónico más pequeños. Por ejemplo, es posible que funcionen bien si realiza envíos a un pequeño grupo de destinatarios bien definido cuyos servidores de correo electrónico aceptan o rechazan correo electrónico a través de una lista de direcciones IP específicas, en lugar de la reputación de la dirección IP.

Costos adicionales

Direcciones IP compartidas: incluidas en el precio estándar de SES.

Direcciones IP dedicadas (estándar): están disponibles a una tarifa mensual adicional por cada dirección IP que se alquila. Para obtener información acerca de los precios, consulte la página de precios de SES.

Direcciones IP dedicadas (administradas): están disponibles a una tarifa mensual estándar (independientemente de la cantidad de IP necesarias) y un cargo por uso de mensajes. Para obtener información acerca de los precios, consulte la página de precios de SES.

Control sobre la reputación del remitente

Direcciones IP compartidas: SES controla su reputación de remitente.

Direcciones IP dedicadas (estándar) | Direcciones IP dedicadas (administradas): su reputación de remitente está totalmente bajo su control. Al utilizar direcciones IP dedicadas, su cuenta de SES es la única que puede enviar correo electrónico desde dichas direcciones. Por este motivo, la reputación del remitente se determina en función de sus prácticas de envío de correos electrónicos. Además, las IP dedicadas (administradas) supervisan activamente las direcciones IP salientes que se utilizan para enviar correo electrónico mediante el uso de las direcciones IP de mayor rendimiento para mejorar la capacidad de entrega del correo electrónico a los destinatarios. Los datos de uso se pueden mostrar mediante servicios adicionales, como CloudWatch las métricas de Amazon y los paneles integrados que se encuentran en Amazon SES.

Capacidad de aislar la reputación del remitente

Direcciones IP compartidas: su reputación de remitente se establece a nivel de cuenta y no se puede aislar.

Direcciones IP dedicadas (estándar) | Direcciones IP dedicadas (administradas): puede aislar su reputación de remitente para distintos componentes en su programa de correo electrónico mediante la creación de grupos de direcciones IP dedicadas, es decir, conjuntos de direcciones IP dedicadas que se pueden utilizar para enviar determinados tipos de correos electrónicos. Por ejemplo, puede crear un conjunto de direcciones IP dedicadas para el envío de correo electrónico de marketing y otro para el envío de correos electrónicos de transacciones.

Direcciones IP conocidas y sin cambios

Direcciones IP compartidas: usted no conoce las direcciones IP que utiliza SES para enviar su correo, y estas pueden cambiar en cualquier momento.

Direcciones IP dedicadas (estándar): puede encontrar los valores de las direcciones que envían su correo en la página Dedicated IPs (IPs dedicadas) de la consola de SES. Esto se debe a que las direcciones IP dedicadas son estáticas.

Direcciones IP dedicadas (administradas): SES configura automáticamente la cantidad óptima de direcciones IP dedicadas en función de sus patrones de envío. Esto significa que las direcciones IP dedicadas de su grupo no son visibles y aumentarán o disminuirán dinámicamente en función de la demanda.

Direcciones IP dedicadas (estándar) en Amazon SES

Las direcciones IP dedicadas (estándar) son direcciones IP dedicadas que se configuran y administran manualmente en SES. Son diferentes de las que se configuran y administran automáticamente mediante la característica the section called “Administradas” de SES. Además de darle el control total de su reputación de envío mediante direcciones IP dedicadas, las IP dedicadas (estándar) le permiten administrar por completo sus IP dedicadas, lo que incluye prepararlas, escalarlas y administrar grupos de IP.

Tanto las IP dedicadas (estándar) como las IP dedicadas (administradas) se refieren a direcciones IP dedicadas que se alquilan en SES por un precio adicional, pero difieren en la forma en que se implementan y administran. Si bien ambos tipos comparten una serie de beneficios, cada uno tiene unas ventajas únicas que ofrecer según el tipo de envío de correo electrónico, tal y como se explica en Direcciones IP dedicadas.

En los temas de esta sección, se explica cómo configurar y administrar manualmente las IP dedicadas (estándar) en SES.

Temas

- Solicitud y renuncia de direcciones IP dedicadas (estándar)
- Preparación de direcciones IP dedicadas (estándar)
- Creación de grupos de IP dedicadas estándar para IP dedicadas (estándar)

Solicitud y renuncia de direcciones IP dedicadas (estándar)

Para utilizar direcciones IP dedicadas (estándar), primero debe solicitarlas. Cuando ya no las necesite, debe renunciar a ellas. Solicite y renuncie a direcciones IP dedicadas (estándar) a través del Centro de AWS Support. Se le cobrará en su cuenta una cuota mensual adicional por cada dirección IP dedicada estándar que alquile para utilizarla con Amazon SES. No hay un compromiso mínimo sobre el uso de IP dedicadas (estándar).

Para obtener más información acerca de los costos asociados con IP dedicadas (estándar), consulte Precios de Amazon SES.

Para obtener una lista de todas las regiones en las que Amazon SES se encuentra actualmente disponible, consulte Región de AWS y puntos de conexión en la Referencia general de Amazon Web Services. Para obtener más información sobre la cantidad de zonas de disponibilidad que hay en cada Región de AWS, consulte Infraestructura global de AWS.

Solicitud de IP dedicadas (estándar)

Para solicitar tantas IP dedicadas (estándar) como necesite, cree un caso de aumento de la Service Quota en el Centro de soporte de AWS.

Para solicitar IP dedicadas (estándar)

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación de la izquierda, elija Dedicated IPs (IP dedicadas).
3. Haga una de las siguientes acciones:

   a. Si no tiene IP dedicadas existentes en la cuenta:

      - Se mostrará la página de incorporación Dedicated IPs (IP dedicadas). En el panel Dedicated IPs (standard) overview (Información general de IP dedicadas [estándar]), elija Request dedicated IPs (Solicitar IP dedicadas).

        Se abrirá la página Create case (Crear caso) en la consola de AWS Support.

   b. Si tiene IP dedicadas existentes en la cuenta:

      i. Seleccione la pestaña Standard IP pools (Grupos de IP estándar) en la página Dedicated IPs (IP dedicadas).

      ii. En el panel Standard overview (Descripción general de Estándar), elija Request or relinquish Standard dedicated IPs (Solicitar o renunciar a IP dedicadas estándar).

        Se abrirá la página Create case (Crear caso) en la consola de AWS Support.
4. En Create case (Crear caso), seleccione la tarjeta Service limit increase (Aumento del límite de servicio) en la parte superior de la página.
5. En Case details (Detalles del caso), complete las secciones siguientes:

   - En Limit type (Tipo de límite), mantenga SES Service Limits (Cuotas de servicio SES).
   - En Mail Type (Tipo de correo), elija el tipo de correo electrónico que prevé enviar mediante la dirección IP dedicada. Si son aplicables varios valores, elija la opción que se aplique a la mayoría del correo electrónico que vaya a enviar.
   - En Website URL (URL del sitio web), escriba la dirección URL de su sitio web. Esta información nos ayuda a entender mejor el tipo de contenido que desea enviar.

- En Describe in detail how you will only send to recipients who have specifically requested your mail (Describa en detalle cómo enviará el correo solo a los destinatarios que lo hayan solicitado específicamente), proporcione una respuesta consistente con su caso de uso.
- En Describe the process that you will follow when you receive bounce and complaint notifications (Describa el proceso que seguirá cuando reciba notificaciones de devoluciones y reclamaciones), proporcione una respuesta consistente con su caso de uso.
- En Will you comply with AWS Service Terms and AUP (¿Cumplirá con las condiciones de servicio de y AUP?), elija la opción que se aplica a su caso de uso.

6. En Requests (Solicitudes), complete las secciones siguientes:

   - En Region (Región), elija la Región de AWS a la que se aplica su solicitud.
   - En Limit (Límite), mantenga Desired Dedicated IP (IP dedicada deseada).
   - En New limit value (Nuevo valor límite), introduzca el número de direcciones IP dedicadas que necesita para implementar su caso de uso.

   > **Note**
   >
   > Si desea solicitar direcciones IP dedicadas para utilizarlas en otra Región de AWS, elija Add another request (Añadir otra solicitud) y, a continuación, complete los campos Region (Región), Limit (Límite) y New limit value (Nuevo valor de límite) para la Región de AWS adicional. Repita este proceso para cada Región de AWS en la que desea utilizar direcciones IP dedicadas.

7. En Case descripción (Descripción del caso), indique en Use case description (Descripción del caso de uso) que desea solicitar direcciones IP dedicadas. Si desea solicitar un número específico de direcciones IP dedicadas, indíquelo también. Si no especifica un número de direcciones IP dedicadas, le proporcionaremos el número de ellas que se necesitan para cumplir el requisito de ratio de envío que ha especificado en el paso anterior.

   A continuación, describa cómo tiene previsto utilizar las direcciones IP dedicadas para enviar correo electrónico mediante Amazon SES. Incluya información acerca de por qué desea usar direcciones IP dedicadas en lugar de direcciones IP compartidas. Esta información nos ayuda a comprender mejor su caso de uso.

8. En Contact options (Opciones de contacto), elija en Preferred contact language (Idioma de contacto preferido) si prefiere recibir las comunicaciones de este caso en English (Inglés) o Japanese (Japonés).

9. Cuando haya terminado, elija Submit (Enviar).

Una vez que envíe el formulario, evaluaremos su solicitud. Si acaptamos su solicitud, responderemos a su caso en el Centro de soporte para confirmarle que sus nuevas direcciones IP dedicadas están asociadas a su cuenta.

Renuncia a direcciones IP dedicadas estándar

Si utiliza direcciones IP dedicadas y ya no quiere que se asocien a tu cuenta, el siguiente procedimiento muestra cómo renunciar a ellas creando un caso en el Centro de soporte de AWS.

> **Important**
>
> El proceso de renuncia a una dirección IP dedicada no se puede revertir. Si renuncia a una dirección IP dedicada en mitad de un mes, prorratearemos la cuota de uso mensual de la dirección IP dedicada, según el número de días del mes actual que hayan transcurrido.

Para renunciar a direcciones IP dedicadas (estándar)

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación de la izquierda, elija Dedicated IPs (IP dedicadas).
3. Seleccione la pestaña Standard IP pools (Grupos de IP estándar) en la página Dedicated IPs (IP dedicadas).
4. En el panel Standard overview (Descripción general de Estándar), elija Request or relinquish Standard dedicated IPs (Solicitar o renunciar a IP dedicadas estándar).
5. En Case details (Detalles del caso), en Limit type (Tipo de límite), mantenga SES Service Limits (Límites de servicio de SES).

   > **Note**
   >
   > Los cuadros restantes de esta sección no se aplican a la renuncia a IP dedicadas. Puede dejarlos en blanco.

6. En Requests (Solicitudes), complete las secciones siguientes:

   - En Region (Región), elija la Región de AWS a la que se aplica su solicitud de renuncia.

> **Note**
>
> Las direcciones IP dedicadas son únicas para cada Región de AWS, por lo que es importante elegir la Región de AWS a la que está asociada la dirección IP dedicada.

- En Limit (Límite), mantenga Desired Dedicated IP (IP dedicada deseada).
- En New limit value (Nuevo valor de límite), escriba cualquier valor. El número que ingrese aquí no es importante, ya que especifica la cantidad de direcciones IP dedicadas a las que desea renunciar en el siguiente paso.

> **Note**
>
> Una misma dirección IP dedicada únicamente se puede utilizar en una sola Región de AWS. Si desea renunciar a direcciones IP dedicadas que utilizó en otras Regiones de AWS, elija Add another request (Añadir otra solicitud). A continuación, complete los campos Region (Región), Limit (Límite) y New limit value (Nuevo valor de límite) de la Región de AWS adicional. Repita este proceso para cada dirección IP dedicada a la que desee renunciar.

7. En Case Descripción (Descripción del caso), indique en Use case description (Descripción del caso de uso) que desea renunciar a direcciones IP dedicadas existentes. Si actualmente tiene alquiladas más de una dirección IP dedicada, incluya el número de direcciones IP a las que desea renunciar.
8. En Contact options (Opciones de contacto), elija en Preferred contact language (Idioma de contacto preferido) si prefiere recibir las comunicaciones de este caso en English (Inglés) o Japanese (Japonés).
9. Cuando haya terminado, elija Submit (Enviar).

Una vez que recibamos su solicitud, le enviaremos un mensaje para pedirle que confirme que desea renunciar a sus direcciones IP dedicadas. Una vez que haya confirmado que desea renunciar a las direcciones IP, las quitaremos de su cuenta.

Preparación de direcciones IP dedicadas (estándar)

A la hora de determinar si desea aceptar o rechazar un mensaje, los proveedores de servicios de correo electrónico tienen en cuenta la dirección IP que lo envía. Uno de los factores que contribuye a la reputación de una dirección IP es si esta tiene un historial de envío de correo electrónico de alta calidad. Es menos probable que los proveedores de correo electrónico acepten correo de nuevas direcciones IP que tengan poco o ningún historial. El correo electrónico enviado desde direcciones IP con poco o ningún historial podría acabar en las carpetas de correo no deseado de los destinatarios o bloquearse.

Cuando empiece a enviar correo electrónico desde una nueva dirección IP dedicada, debe aumentar gradualmente la cantidad de correo electrónico que envía desde esa dirección antes de utilizarla a plena capacidad. Este proceso se denomina preparación de la dirección IP.

La cantidad de tiempo necesario para preparar una dirección IP varía en función del proveedor de correo electrónico. Para algunos proveedores de correo electrónico, puede establecer una reputación positiva en aproximadamente dos semanas, mientras que para otros puede tardar hasta seis semanas. Cuando prepare una nueva dirección IP dedicada, debe enviar correo electrónico a los usuarios más activos para garantizar que la tasa de reclamaciones permanezca baja. También debe examinar atentamente los mensajes de rebotes y enviar menos correo electrónico si recibe un gran número de notificaciones de bloqueo o limitación. Para obtener información sobre cómo monitorizar los rebotes, consulte Monitoreo de la actividad de envío de Amazon SES.

Preparación automática para IP dedicadas (estándar)

Cuando solicita direcciones IP dedicadas (estándar), Amazon SES las prepara automáticamente para mejorar la entrega del correo electrónico que envía. La característica de preparación automática de direcciones IP está activada de forma predeterminada. SES prepara automáticamente sus IP dedicadas aumentando gradualmente la cantidad de correos electrónicos que envía a través de sus IP dedicadas en función de un plan de preparación predefinido. La cantidad máxima diaria de correos aumenta desde el primer día hasta que alcanza un máximo de 50 000 correos electrónicos en un plazo de 45 días. Este aumento gradual ayuda a sus IP a conseguir una buena reputación entre los proveedores de servicios de Internet (ISP).

Los pasos que se realizan durante el proceso de preparación automática dependen de si ya dispone o no de direcciones IP dedicadas.

- Cuando solicita IP dedicadas (estándar) por primera vez, SES distribuye el envío de correo electrónico entre sus direcciones IP dedicadas y un conjunto de direcciones que se comparten con

otros clientes de SES. SES aumenta gradualmente el número de mensajes que se envían desde las direcciones IP dedicadas con el paso del tiempo.

- Si ya tiene direcciones IP dedicadas, SES distribuye el envío de correo electrónico entre sus direcciones IP dedicadas (si ya están preparadas) y las nuevas direcciones IP dedicadas (que no están preparadas). SES aumenta gradualmente el número de mensajes que se envían desde las nuevas direcciones IP dedicadas con el paso del tiempo.

> **Note**
>
> La preparación automática de IP es un proceso basado en el tiempo. El porcentaje de preparación aumenta de forma constante durante 45 días, sin importar el volumen de envío.

Después de preparar una dirección IP dedicada, debe enviar aproximadamente 1 000 mensajes de correo electrónico cada día a cada proveedor de correo electrónico con el que desee mantener una reputación positiva. Debe realizar esta tarea en cada dirección IP dedicada que utilice con SES.

Debe procurar no enviar grandes volúmenes de correo electrónico inmediatamente después de que termine el proceso de preparación. En lugar de ello, aumente lentamente el número de mensajes que envía hasta alcanzar el volumen deseado. Si un proveedor de correo electrónico detecta un gran aumento repentino en el número de mensajes enviados desde una dirección IP, podría bloquear o limitar la entrega de mensajes desde esa dirección.

Deshabilitar el proceso de preparación automático en IP dedicadas (estándar)

Cuando adquiere nuevas direcciones IP dedicadas estándar, Amazon SES las prepara automáticamente, porque la característica de preparación automática de direcciones IP está habilitada de manera predeterminada para su cuenta. Si prefiere preparar usted mismo las direcciones IP dedicadas, puede deshabilitar la característica de preparación automática al nivel de cuenta para todas sus direcciones IP.

Si deshabilita la característica de preparación automática, cualquier IP dedicada que se alquile posteriormente se añadirá a su cuenta con el estado de preparación Complete (Completada), lo que se podrá utilizar sin prepararla; eso significa que usted es el responsable de asegurarse de que estas IP se preparen correctamente antes de usarlas para los envíos regulares. No se utilizará ninguna IP que se encuentre en fase de preparación en el momento en que deshabilitó la función de preparación automática.

> **Important**
>
> Si desactiva la característica de preparación automática, usted es responsable de preparar las direcciones IP dedicadas. Si envía correo electrónico desde direcciones que no se han preparado, puede experimentar tasas de envío reducidas.

Para deshabilitar (o volver a habilitar) la característica de preparación automática para todas las IP dedicadas (estándar) de su cuenta

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación de la izquierda, elija Dedicated IPs (IP dedicadas).
3. Seleccione la pestaña Standard IP pools (Grupos de IP estándar) en la página Dedicated IPs (IP dedicadas).
4. Seleccione Disable auto warm-up (Deshabilitar preparación automática) en el panel Standard overview (Descripción general estándar) para deshabilitar la preparación automática, o seleccione Enable auto warm-up (Habilitar preparación automática) para volver a habilitar la preparación automática.

Preparación manual de las direcciones IP dedicadas (estándar)

Puede aumentar o disminuir manualmente el volumen de envío actual de sus IP dedicadas (estándar) editando su porcentaje de preparación, puede finalizar el proceso de preparación prematuramente y puede establecer el volumen de envío actual en el 0 % y reiniciar el proceso de preparación.

Para preparar manualmente las direcciones IP dedicadas (estándar)

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación de la izquierda, elija Dedicated IPs (IP dedicadas).
3. Seleccione la pestaña Standard IP pools (Grupos de IP estándar) en la página Dedicated IPs (IP dedicadas).

4. En el panel All Standard dedicated IPs (Todas las IP dedicadas estándar), seleccione una dirección IP y elija Edit warm up (Editar preparación); luego, seleccione una de las siguientes opciones:

   a. Edit percentage (Editar porcentaje): introduzca un valor en el campo Warm-up percentage (Porcentaje de preparación) para aumentar o disminuir el volumen de envío actual de su IP editando su porcentaje de preparación y luego pulse en Save changes (Guardar cambios).

      La columna Warm-up status (Estado de preparación) indicará `In progress` y la columna Warm-up percentage (Porcentaje de preparación) indicará el valor que ha introducido.

   b. Mark as Complete (Marcar como completado): lea el cuadro de diálogo Mark warm-up as Complete? (¿Marcar preparación como completada?) para confirmar que comprende las consecuencias que tiene finalizar el proceso de preparación automática de forma prematura y, a continuación, seleccione Mark as Complete (Marcar como completado).

      La columna Warm-up status (Estado de preparación) indicará `Complete` y la columna Warm-up percentage (Porcentaje de preparación) indicará `100%`.

   c. Reset percentage (Restablecer porcentaje): lea el cuadro de diálogo Reset warm-up percentage? (¿Restablecer porcentaje de preparación?) para confirmar que está configurando el volumen de envío actual de IP en 0 %. Tendrá que reiniciar el proceso de preparación automática o configurar el porcentaje de preparación manualmente y, a continuación, elegir Reset (Restablecer).

      La columna Warm-up status (Estado de preparación) indicará `In progress` y la columna Warm-up percentage (Porcentaje de preparación) indicará `0%`.

Creación de grupos de IP dedicadas estándar para IP dedicadas (estándar)

Si ha adquirido varias direcciones IP dedicadas (estándar) para utilizarlas con Amazon SES, puede crear grupos de dichas direcciones, que se denominan grupos de IP dedicadas. Al agrupar las IP dedicadas (estándar) en un grupo, es más fácil administrarlas. Un escenario común consiste en crear un grupo para enviar comunicaciones de marketing y otro para enviar correos electrónicos de transacciones. Su reputación de remitente para correos electrónicos de transacciones queda aislada de la de sus correos electrónicos de marketing. En este caso, si una campaña de marketing genera un gran número de reclamaciones, la entrega de sus correos electrónicos de transacción no se verá afectada.

Esta sección contiene procedimientos para crear grupos de IP dedicadas.

> **Note**
>
> También puede crear conjuntos de configuraciones que utilicen un grupo de direcciones IP que compartan todos los clientes de SES. El grupo de IP compartidas resulta útil en situaciones en las que necesita enviar un correo electrónico que no se ajuste a las situaciones habituales. Para obtener información acerca de cómo utilizar el grupo de IP compartidas con un conjunto de configuración, consulte Asignación de grupos de IP en Amazon SES.

Para crear un grupo de IP dedicadas para IP dedicadas (estándar) mediante la consola de SES

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación de la izquierda, elija Dedicated IPs (IP dedicadas).

   > **Note**
   >
   > Si actualmente no tiene ninguna IP dedicada (estándar) en la cuenta, se mostrará la página de incorporación Dedicated IPs (IP dedicadas), que le permitirá comprar IP dedicadas (estándar). Para obtener más información, consulte the section called “Solicitud de IP dedicadas (estándar)”.

3. Seleccione la pestaña Standard IP pools (Grupos de IP estándar) en la página Dedicated IPs (IP dedicadas).
4. En el panel All Dedicated IP (standard) pools (Todos los grupos de IP dedicadas [estándar]), elija Create Standard IP pool (Crear grupo de IP estándar).

   Se abrirá la página Create IP Pool (Crear grupo de direcciones IP).
5. En el panel Pool details (Detalles de grupo):

   a. Elija Standard (self managed) (Estándar [Autoadministrado]) en el campo Scaling mode (Modo de escalado).

   b. Introduzca un nombre para su grupo de direcciones IP en el campo IP pool name (Nombre del grupo de IP).

> **Note**
>
> El nombre del grupo de IP debe ser único y no puede ser un duplicado del nombre de un grupo de IP administradas de su cuenta.

c. (Opcional) Si tiene direcciones IP dedicadas estándar que desea añadir a este conjunto de IP, selecciónelas en la lista desplegable del campo Dedicated IP addresses (Direcciones IP dedicadas).

> **Note**
>
> Si selecciona una dirección IP que ya está asociada a un grupo de IP, ahora solo se asociará a este grupo de IP.

6. (Opcional) Puede asociar este grupo de IP a un conjunto de configuraciones seleccionando una en la lista desplegable del campo Configuration sets (Conjuntos de configuraciones).

> **Note**
>
> - Si selecciona un conjunto de configuraciones que ya está asociado a un conjunto de IP, ahora solo se asociará a este conjunto de IP.
> - Para añadir o eliminar conjuntos de configuraciones asociados después de crear este grupo de IP, edite el parámetro Sending IP pool (Grupo de IP de envío) del conjunto de configuraciones.
> - Si aún no ha creado ningún conjunto de configuración, consulte Conjuntos de configuración.

7. (Opcional) Puede añadir una o varias etiquetas a este grupo de IP. Para ello, incluya una clave de etiqueta y un valor opcional para la clave.

   a. Elija Add new tag (Agregar nueva etiqueta) e ingrese la Key (Clave). También puede agregar un valor opcional para la etiqueta.

   b. Para agregar la etiqueta, elija Save changes (Guardar los cambios).

   Puede añadir hasta 50 etiquetas. Para eliminar una etiqueta, elija la opción Remove (Eliminar).

8. Seleccione Create Pool (Crear grupo).

> **Note**
>
> Después de crear un grupo de IP estándar, tiene la opción de convertirlo en un grupo de IP administradas. Consulte Creación de un grupo de IP administradas.

Direcciones IP dedicadas (administradas) para Amazon SES

Las direcciones IP dedicadas (administradas) son una característica de Amazon SES que configura y administra automáticamente las direcciones IP dedicadas en su nombre para proporcionarle una forma rápida y sencilla de empezar a utilizar direcciones IP dedicadas que administra SES. Esto ayuda a garantizar que sus direcciones IP dedicadas se utilicen de una manera eficiente y óptima para enviar correos electrónicos.

Para habilitar las IP dedicadas (administradas) en la cuenta, se crea un grupo de IP administradas y SES se encarga de todo lo demás. SES determinará cuántas IP dedicadas necesita en función de los patrones de envío, las creará por usted y, a continuación, gestionará su escalabilidad en función de los requisitos de envío.

Una vez habilitadas, puede utilizar las IP dedicadas (administradas) para el envío de correos electrónicos asociando el grupo de IP administradas a un conjunto de configuración y, a continuación, especificando ese conjunto de configuración al enviar los correos electrónicos. El conjunto de configuraciones también se puede aplicar a una identidad de envío mediante un conjunto de configuraciones predeterminado.

Beneficios y características de las IP dedicadas (administradas)

Las direcciones IP dedicadas que crea con IP dedicadas (administradas) automatizan las tareas de administración para garantizar que sus direcciones IP dedicadas se utilicen de la manera óptima para enviar correos electrónicos:

- Incorporación sencilla: para empezar a utilizar IP dedicadas (administradas), debe crear un grupo de direcciones IP administradas directamente desde la consola de SES. Las direcciones IP dedicadas se asignan automáticamente al grupo. Puede empezar a enviar con el grupo de direcciones IP gestionado sin tener que abrir un caso de solicitud a través del AWS Support Center.

- Escalado automático por ISP: no es necesario que supervise ni escale manualmente sus grupos de IP dedicados, ya que el grupo de IP administrado se amplía automáticamente en función del uso. También tiene en cuenta las políticas específicas del ISP. Por ejemplo, si SES detecta que un ISP admite una cuota de envío diaria baja, el grupo se escala horizontalmente para distribuir mejor el tráfico a ese ISP entre más direcciones IP.
- Preparación inteligente: las IP dedicadas (administradas) comienzan a enviar correo a los ISP en función de su capacidad. Es decir, de cuánto están preparadas en ese momento. Realizan un seguimiento automáticamente del nivel de preparación de cada ISP de forma individual. Además, la función de direcciones IP dedicadas (gestionadas) proporciona información sobre tu reputación a un ritmo diario efectivo con los principales ISP en forma de CloudWatch métricas de Amazon y paneles integrados.
  - Preparación por ISP: SES realiza un seguimiento de la reputación de cada IP en el grupo de direcciones IP administradas para cada ISP de forma individual. Por ejemplo, si ha estado enviando todo su tráfico a Gmail, las direcciones IP se consideran preparadas solo para Gmail, no para otros ISP. Si cambia su patrón de tráfico aumentando el correo electrónico que envía a Hotmail, SES aumentará el tráfico lentamente para Hotmail, ya que las direcciones IP aún no se han preparado.
  - Calentamiento adaptativo y transición a piscinas compartidas: el ajuste de calentamiento es adaptativo y tiene en cuenta los patrones de envío reales. Cuando el volumen de envío a un ISP disminuye, el porcentaje de preparación también disminuye para ese ISP. En la fase inicial del calentamiento, cualquier envío que sea excesivo en función del nivel actual de calentamiento se envía a través de las direcciones IP que se comparten con otros usuarios de Amazon SES (el grupo compartido de SES). En fases posteriores de la preparación, cualquier envío que sea excesivo se ralentiza de forma proactiva y se vuelve a intentar más adelante.

    Important

    Si bien las IP dedicadas (administradas) calientan automáticamente las direcciones IP dedicadas, parte de ese proceso automático consiste en trabajar de forma interactiva con el conjunto de IP compartidas de SES.

    - Si su tasa de envío es demasiado alta para sus nuevas IP dedicadas mientras se están calentando, SES transferirá automáticamente parte de sus envíos al conjunto de direcciones IP compartidas de SES para proteger la reputación de sus nuevas IP dedicadas.
    - Incluso después de que tus nuevas IP dedicadas se hayan calentado por completo, no se garantiza que todos tus envíos se realicen a través de ellas el 100% del tiempo.

Por ejemplo, si tu velocidad de envío aumenta repentinamente y las IP dedicadas (administradas) determinan que deben asignar una dirección IP dedicada adicional, se iniciará el proceso de calentamiento, que incluye el uso del pool compartido. Del mismo modo, si tu tasa de envío cae repentinamente a un nivel muy bajo, todos tus envíos podrían pasar al conjunto de direcciones IP compartidas de SES, consulte. the section called “Importancia de la preparación”

- Solicitud y cesión automáticas de direcciones IP dedicadas: no es necesario que solicite ni ceda direcciones IP dedicadas administradas a través del AWS Support Center, como ocurre cuando se utilizan direcciones IP dedicadas (estándar). Al realizar la incorporación con IP dedicadas (administradas) directamente desde la consola, la CLI o la API de SES, se le asignan automáticamente direcciones IP dedicadas y se le cobra una tarifa en función del volumen de mensajes que envíe. Cuando elimina un grupo de IP creado por IP dedicadas (administradas) o cancela las IP dedicadas (administradas), renuncia automáticamente a las direcciones IP asignadas y se le dejan de cobrar los cargos de inmediato.
  - Obtener la primera dirección IP dedicada: la función IP dedicada (administrada) asignará automáticamente su primera dirección IP dedicada una vez que el volumen de envíos alcance cientos de correos electrónicos en un plazo de unos pocos días. Esto garantiza que la IP desde la que envía pueda generar una reputación de envío y mejorar la capacidad de entrega. (Si no espera que su volumen de envío esté en este nivel, debe utilizar direcciones IP compartidas. Consulte la tabla comparativa en Direcciones IP dedicadas para ver el tipo de direcciones IP que mejor se adaptan a la forma de enviar correos electrónicos.)

Por qué es importante una preparación adecuada de la IP

Para garantizar que su correo electrónico se entregue a través de su dirección IP dedicada, debe tener una buena reputación para el ISP receptor. Los ISP solo aceptarán un pequeño volumen de correo electrónico de una IP que no reconozcan. Cuando se le asigna una IP por primera vez, es nueva y el ISP receptor no la reconoce porque no tiene reputación asociada. Para establecer la reputación de una IP, debe generar gradualmente confianza con el ISP receptor; este proceso gradual de creación de confianza se denomina preparación. Inmediatamente después de que las IP dedicadas (administradas) asignen una IP, se inicia el proceso de preparación inteligente.

Con las funciones Preparación por ISP y Preparación adaptativa de las IP dedicadas (administradas), la continuidad empresarial se mantiene durante todo el ciclo de preparación al garantizar la entrega del correo electrónico. Una vez finalizada la fase de preparación, cualquier exceso de capacidad se pone en cola y se envía únicamente a través del grupo de IP dedicado. Sin embargo, si tienes una

dirección IP dedicada y tus envíos están por debajo del volumen mínimo necesario para mantener la reputación IP, las IP dedicadas (administradas) pueden eliminar tu IP dedicada y tus envíos se enrutarán a través del conjunto de IP compartidas de SES.

> **Note**
>
> Si envía pequeños volúmenes de correo electrónico (menos de unos pocos cientos al día durante unos días), sería más beneficioso enviarlos a través del grupo de direcciones IP compartidas de SES. Para comprobar si las IP dedicadas (administradas) son adecuadas para enviar correo electrónico, consulte la tabla comparativa en Direcciones IP dedicadas.

Creación de un grupo de IP administradas para habilitar IP dedicadas (administradas)

Para habilitar las IP dedicadas (administradas), debe crear primero un grupo de IP administradas. Después de crear un grupo administrado, la función determina cuántas IP dedicadas necesita en función de los patrones de envío y escalará dinámicamente de acuerdo con los requisitos.

Para usar el grupo administrado para enviar correo electrónico, debe asociarlo a un configuration set (conjunto de configuración) y, a continuación, especificar ese conjunto de configuración al enviar el correo electrónico. El conjunto de configuraciones también se puede aplicar a una identidad de envío mediante un conjunto de configuraciones predeterminado.

Hay dos formas de crear un grupo de IP administradas:

- Cree un nuevo grupo.
- Convierta un grupo existente estándar en administrado.

En los procedimientos siguientes, se proporcionan instrucciones para cualquiera de los métodos.

Para crear o convertir un grupo de IP administradas mediante la consola de SES

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. En el panel de navegación de la izquierda, elija Dedicated IPs (IP dedicadas).
3. En función de si desea crear un nuevo grupo de IP administradas o convertir un grupo de IP dedicadas estándar en uno administrado, siga las instrucciones correspondientes:

Create new pool

Para crear un nuevo grupo de IP administradas

1. Realice una de las acciones siguientes:

   a. Si no tiene IP dedicadas existentes en la cuenta:

      - Se mostrará la página de incorporación Dedicated IPs (IP dedicadas). En el panel Dedicated IPs (managed) overview (Información general de IP dedicadas [administradas]), elija Enable dedicated IPs (Habilitar IP dedicadas).

        Se abrirá la página Create IP Pool (Crear grupo de direcciones IP).

   b. Si tiene IP dedicadas existentes en la cuenta:

      i. Seleccione la pestaña Managed IP pools (Grupos de IP administradas) en la página Dedicated IPs (IP dedicadas).

      ii. En el panel All Dedicated IP (managed) pools (Todos los grupos de IP dedicadas [administradas]), elija Create Managed IP pool (Crear grupo de IP administradas).

        Se abrirá la página Create IP Pool (Crear grupo de direcciones IP).

2. En el panel Pool details (Detalles de grupo):

   a. Elija Managed (auto managed) (Administrado [autoadministrado]) en el campo Scaling mode (Modo de escalado).

   b. Introduzca un nombre para su grupo administrado en el campo IP pool name (Nombre del grupo de IP).

> **Note**
>
> - El nombre del grupo de IP debe ser único. No puede ser un duplicado del nombre de un grupo de IP dedicado estándar de su cuenta.
> - No puede tener más de 50 grupos de IP dedicadas por Región de AWS en la cuenta, incluidos los grupos de IP administrados y estándar.

3. (Opcional) Puede asociar este grupo de IP administradas a un conjunto de configuraciones seleccionando una en la lista desplegable del campo Configuration sets (Conjuntos de configuraciones).

> **Note**
>
> - Si elige un conjunto de configuraciones que ya esté asociado a un grupo de IP, se asociará a este grupo administrado y dejará de estar asociado al grupo anterior.
> - Para añadir o eliminar conjuntos de configuraciones asociados después de crear este grupo administrado, edite el parámetro Sending IP pool (Grupo de IP de envío) del conjunto de configuraciones en el panel General details (Detalles generales).
> - Si aún no ha creado ningún conjunto de configuración, consulte Conjuntos de configuración.

4. (Opcional) Puede agregar una o varias etiquetas a su grupo de IP. Para ello, incluya una clave de etiqueta y un valor opcional para la clave.

   a. Elija Add new tag (Agregar nueva etiqueta) e ingrese la Key (Clave). También puede agregar un valor opcional para la etiqueta. Puede agregar hasta 50 etiquetas. Si comete un error, elija Remove (Eliminar).

   b. Para agregar las etiquetas, elija Save changes (Guardar los cambios).

      Después de crear el grupo, puede agregar, eliminar o editar las etiquetas, seleccionando el grupo administrado y eligiendo Edit (Editar).

5. Seleccione Create Pool (Crear grupo).

> **Note**
>
> - Después de crear un grupo de IP administradas, este no se puede convertir en un grupo de IP estándar.
> - Al utilizar direcciones IP dedicadas (administradas), no puede tener más de 10 000 identidades de envío (dominios y direcciones de correo electrónico, Región de AWS en cualquier combinación) por cuenta.

Convert standard to managed

Para convertir un grupo de IP dedicadas estándar en administrado

1. Seleccione la pestaña Standard IP pools (Grupos de IP estándar) en la página Dedicated IPs (IP dedicadas).
2. En el panel Todos los grupos de IP dedicados (estándar), seleccione la casilla de verificación del grupo de IP dedicadas que desee convertir de estándar a administrado.
3. Elija Convertir en grupo administrado: lea el cuadro de diálogo Convertir en grupo de IP administrado para confirmar que comprende las condiciones para convertir el grupo de IP dedicadas estándar en uno administrado.

> **Note**
>
> Antes de convertir el grupo de IP dedicadas de estándar en administrado, tenga en cuenta lo siguiente:
>
> 1. Todas las IP dedicadas actuales (estándar) se moverán al grupo administrado.
> 2. Si actualmente alquila demasiadas IP dedicadas (estándar) para el volumen de envíos, las IP dedicadas (administradas) eliminarán las IP redundantes.
> 3. Si alguna de las IP dedicadas (estándar) forma parte de una lista de permitidos para otras aplicaciones, no debe transferirla al grupo administrado, ya que se eliminará si se vuelven redundantes; consulte el punto 2.
> 4. Ya no se le cobrará por IP, sino que se le cobrará en función del volumen que envíe a través del grupo administrado. Consulte Precios de Amazon SES.

4. Si está de acuerdo con las condiciones indicadas, elija Confirmar; aparecerá un banner que confirma que el grupo de IP dedicadas estándar se ha convertido en un grupo administrado.

> **Note**
>
> Todos los conjuntos de configuraciones o etiquetas que tenía asociados al grupo estándar antes de la conversión ahora se asociarán al grupo administrado, lo

que proporciona una transición fluida para cualquier envío de correo electrónico mediante el conjunto de configuraciones.

La publicación de eventos se puede utilizar para realizar un seguimiento del rendimiento de envío del grupo administrado. Para obtener más información, consulte the section called “Supervisar el envío de correo electrónico mediante la publicación de eventos”.

Visualización del envío y la capacidad del grupo de IP administradas en la consola de Amazon SES

Para los grupos de IP administradas que ha creado, la consola de SES le proporciona una forma sencilla de observar cómo se utilizan para enviar correos electrónicos mediante el uso de tarjetas y gráficos de series temporales que muestran las métricas de envío y la utilización y la capacidad del ISP.

Para ver el envío y la capacidad del grupo de IP administradas mediante la consola de SES

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. En el panel de navegación de la izquierda, elija Dedicated IPs (IP dedicadas).
3. Seleccione la pestaña Managed IP pools (Grupos de IP administradas) en la página Dedicated IPs (IP dedicadas).
4. En función de si deseas ver las métricas de envío y capacidad en la consola Amazon SES o en la CloudWatch consola Amazon, sigue las instrucciones correspondientes:

   Amazon SES console

   Para ver las métricas de envío y capacidad en la consola de Amazon SES

   1. En la tabla Todos los grupos de IP dedicados (administrados), seleccione el nombre de un grupo de IP administradas que se muestra en la columna Grupo de IP para ver los detalles.

      La página de detalles del grupo de IP seleccionadas se abre con las siguientes tarjetas y gráficos de series temporales:

      a. Tarjetas:

- Estado del envío: indica si el volumen y la frecuencia de envío son suficientes para utilizar IP dedicadas. Para ello, muestra uno de los dos estados:
  - Volumen insuficiente: el volumen de envíos es demasiado bajo.
  - Envío mediante IP dedicadas: se utilizan una o más IP dedicadas en el grupo administrado.
- Volumen de envío de IP dedicadas administrado: el volumen de correo electrónico enviado a través de las IP dedicadas en el grupo administrado durante los últimos 7 días.
- Porcentaje de envío de IP dedicadas administradas: el porcentaje de correos electrónicos enviados a través de las IP dedicadas del grupo administrado en los últimos 7 días.

b. Gráficos:

- Volumen enviado: el volumen de correo electrónico enviado en los últimos 7 días a través de IP dedicadas administradas, en comparación con las IP compartidas.
- Porcentaje de volumen enviado: el porcentaje de correo electrónico enviado en los últimos 7 días a través de IP dedicadas administradas, en comparación con las IP compartidas.
- Capacidad del ISP: muestra la cantidad de correo electrónico que se envía a través de IP dedicadas en el grupo administrado según los 10 ISP más utilizados y su capacidad disponible durante el envío:
  - Envíos para el ISP (barras rojas): el volumen de correo electrónico que envió en las últimas 24 horas a través del ISP seleccionado.
  - Capacidad del ISP (línea azul): la capacidad disponible del ISP seleccionado durante las últimas 24 horas.

2. Para filtrar por un ISP específico para el gráfico de capacidad del ISP, elija el cuadro de lista de ISP y seleccione un ISP; el gráfico se actualizará con las métricas del ISP seleccionado. (Si no filtra en un ISP, se mostrará Gmail de forma predeterminada).

Amazon CloudWatch console

Para ver las métricas de envío y capacidad en la CloudWatch consola de Amazon

- En la tabla Todos los grupos de IP dedicadas (gestionados), selecciona el <pool_name>enlace Ver CloudWatch métricas de la columna de CloudWatchmétricas para ver sus detalles.

  La página del grupo de IP seleccionado se abre en la CloudWatch consola y muestra las siguientes métricas:

  - Enviar: el volumen de correo electrónico enviado a través de IP dedicadas administradas e IP compartidas.
  - ApproximateDedicatedSendingPercentage— Indica el porcentaje aproximado de tráfico que se ha entregado a través de una IP dedicada.
  - SentLast24 horas: el volumen de correo electrónico que ha enviado en las últimas 24 horas a través del ISP seleccionado. (Envíos para ISP etiquetados en la consola de SES).
  - Disponible24 HourSend: la capacidad disponible del ISP seleccionado durante las últimas 24 horas. (Capacidad para ISP etiquetada en la consola de SES).

Eliminación de un grupo de IP administradas y desactivación de IP dedicadas (administradas)

Al eliminar un grupo de IP administradas, se renuncia automáticamente a todas las direcciones IP asignadas. Si solo tiene un grupo de IP administradas y lo elimina o elimina el último grupo de IP administradas que le quede, desactivará la función de IP dedicadas (administradas) y los cargos cesarán inmediatamente.

Para eliminar un grupo de IP administradas mediante la consola de SES

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. En el panel de navegación de la izquierda, elija Dedicated IPs (IP dedicadas).
3. Seleccione la pestaña Managed IP pools (Grupos de IP administradas) en la página Dedicated IPs (IP dedicadas).

4. En la tabla All Dedicated IP (managed) pools (Todos los grupos de IP dedicadas [administradas]), seleccione el botón de opción situado junto al nombre del IP pool (Grupo de IP) del grupo administrado que desea eliminar y elija Delete (Eliminar).
5. En el modal emergente, tendrá la oportunidad de confirmar la elección seleccionando Delete (Eliminar) o de conservar el grupo administrado haciendo clic en Cancel (Cancelar).

> **Note**
>
> Si solo tiene un grupo administrado o va a eliminar el último grupo administrado, el modal emergente le recordará que, al eliminar el resto del grupo administrado, desactivará la función de IP dedicadas (administradas) y ya no se le cobrará por ella. Para poder elegir Delete (Eliminar), antes tendrá que introducir *`Disable`* en el campo de confirmación.

Uso de sus propias direcciones IP para enviar correo electrónico con Amazon SES

Amazon SES incluye una característica llamada Bring Your Own IP (Traiga su propia IP) (BYOIP), que le permite utilizar sus propias direcciones IP para enviar correo electrónico a través de Amazon SES. Si ya utiliza un intervalo de direcciones IP para enviar correo electrónico, puede solicitar que hagamos que su intervalo de direcciones IP esté disponible para enviar correo electrónico a través de Amazon SES.

> **Note**
>
> BYOIP solo está disponible para direcciones IP dedicadas que se configuran manualmente; no se puede usar con IP dedicadas (administradas).

BYOIP es útil, por ejemplo, cuando ha desarrollado una reputación positiva de sus direcciones IP mediante un sistema interno de envío de correo electrónico, pero desea migrar a Amazon SES. Mediante el uso de BYOIP, puede comenzar a enviar correo electrónico a través de Amazon SES inmediatamente, sin tener que restablecer la reputación de sus direcciones IP.

Requisitos

Para utilizar BYOIP, su intervalo de direcciones IP debe cumplir los siguientes requisitos:

- El intervalo de direcciones debe estar registrado en el Registro Regional de Internet (RIR, por sus siglas en inglés), como, por ejemplo, el Registro Americano de Números de Internet (ARIN, por sus siglas en inglés), el Centro de Coordinación de Redes IP Europeas (RIPE NCC, por sus siglas en francés) o el Centro de Información de Redes de Asia y el Pacífico (APNIC, por sus siglas en inglés). El intervalo de direcciones tiene que estar registrado en una empresa o entidad institucional y no se puede registrar a nombre de una persona.
- Debe poder proporcionar pruebas de que usted es el propietario del intervalo de direcciones enviando un mensaje de autorización firmado.
- Las direcciones del intervalo de direcciones IP deben tener un historial limpio. Podemos investigar la reputación del intervalo de direcciones IP y nos reservarnos el derecho de rechazar un intervalo de direcciones IP si contiene una dirección IP con una mala reputación o que esté asociada a un comportamiento malicioso.
- El intervalo de direcciones IP no puede incluir intervalos de direcciones IP que se han traído a otro Servicio de AWS para BYOIP, como Amazon EC2.

Consideraciones

Hay varios factores que debe tener en cuenta antes de solicitar la transferencia de sus intervalos de direcciones IP a Amazon SES:

- El rango de dirección más específico que puede especificar es /24. En otras palabras, si transfiere el intervalo de IP 203.0.113.0/24 a su cuenta de Amazon SES, puede realizar envíos desde un total de 256 direcciones, comprendidas de 203.0.113.0 a 203.0.113.255. Debe transferir todo el intervalo: Amazon SES no le permite transferir direcciones IP individuales.
- Si utiliza BYOIP para un intervalo específico de direcciones IP, solo puede obtener acceso a ese intervalo desde una única Región de AWS.
- Puede traer cinco intervalos de direcciones por región a su Cuenta de AWS.
- Si utiliza sus propias direcciones IP, no puede utilizar las direcciones del grupo de direcciones IP compartidas de Amazon SES. Si necesita utilizar estas direcciones IP compartidas, puede utilizar Amazon SES en una Región de AWS diferente o crear una nueva Cuenta de AWS.
- Existe un cargo mensual por cada dirección IP que se utiliza con BYOIP. Para obtener más información, consulte precios de Amazon SES.

Uso de sus propias direcciones IP con Amazon SES

Para evitar que nuestros sistemas se utilicen para enviar contenido no solicitado o malicioso, tenemos que considerar cada solicitud BYOIP detenidamente.

Si desea utilizar su propio intervalo de direcciones IP con Amazon SES, envíe la siguiente información a ses-byoip-request@amazon.com:

- Su ID de cuenta de AWS.
- La Región de AWS en la que desea utilizar el intervalo IP, por ejemplo, ap-south-1.
- Una descripción del caso de uso.
- Intervalo de direcciones IP que desea utilizar con Amazon SES.
- Nombre del registro de Internet en el que está registrado el intervalo.

Responderemos a su solicitud en un plazo de 48 horas laborables. En nuestras comunicaciones con usted, le podríamos solicitar información adicional, incluidos documentos que acrediten que usted es el propietario del intervalo de direcciones IP.

Virtual Deliverability Manager para Amazon SES

La capacidad de entrega, es decir, la capacidad de garantizar que los correos electrónicos lleguen a las bandejas de entrada de los destinatarios en lugar de a las carpetas de spam o correo no deseado, es un elemento fundamental para el éxito de una estrategia de correo electrónico.

Virtual Deliverability Manager es una función de Amazon SES que le ayuda a mejorar la capacidad de entrega del correo electrónico, por ejemplo, a aumentar la capacidad de entrega en la bandeja de entrada y las conversiones de correo electrónico, ya que proporciona información sobre los datos de envío y entrega y consejos sobre cómo solucionar los problemas que afectan negativamente a su reputación y a su tasa de éxito de entrega.

Por qué son importantes la capacidad de entrega en la bandeja de entrada y la reputación del remitente

La capacidad de entrega en la bandeja de entrada es un factor clave en lo que respecta a las conversiones de correo electrónico (cuando un destinatario realiza una acción después de abrir un correo electrónico): los clientes que no reciban los mensajes no podrán verlos y, mucho menos, interactuar con ellos.

La reputación de envío es la que más influye en la capacidad de entrega en la bandeja de entrada desde el punto de vista de la experiencia del cliente, ya que determina si los mensajes no deseados llegan a los destinatarios o si los mensajes necesarios se envían a carpetas de correo no deseado o se bloquean antes de poder llegar a los buzones de los destinatarios.

Cómo Virtual Deliverability Manager puede ayudar a mejorar la capacidad de entrega y la reputación

Virtual Deliverability Manager le ayuda a mejorar su capacidad de entrega y su reputación con un panel que ofrece vistas generales y detalladas del programa de correo electrónico de la cuenta para ayudarle a centrarse en las áreas problemáticas, y un asesor que ofrece soluciones a problemas de infraestructura que afectan negativamente a su capacidad de entrega de correo electrónico y su reputación.

- Panel: proporciona información sobre los datos de capacidad de entrega, en concreto los relacionados con la cuenta, el ISP, la identidad de envío y los niveles del conjunto de configuración. Esto le ayuda a ver rápidamente áreas y tendencias problemáticas y a detectar posibles problemas antes de que se conviertan en problemas de capacidad de entrega más importantes, como las denegaciones temporales (aplazamientos) o los bloqueos. Esta información

también le ayudará a mejorar su reputación como remitente al calcular las fechas y horas ideales para aumentar las interacciones de los clientes y las conversiones en las campañas de correo electrónico.

- Asesor: proporciona recomendaciones para mejorar el envío de correos electrónicos al señalar los problemas de configuración que afectan negativamente a su capacidad de entrega de correo electrónico y su reputación. Recomendará soluciones para resolver problemas específicos en la infraestructura del dominio de envío, el espacio IP y los registros de autenticación, por ejemplo, cuando no existan registros de SPF, DMARC o DKIM o si la longitud de la clave DKIM es demasiado corta.

Introducción a Virtual Deliverability Manager

Para empezar a utilizar Virtual Deliverability Manager, un asistente de incorporación de la consola de Amazon SES le indicará los pasos necesarios para habilitar Virtual Deliverability Manager en la cuenta. Consulte the section called “Introducción”.

Temas

- Introducción a Virtual Deliverability Manager
- Panel Virtual Deliverability Manager
- Asesor de Virtual Deliverability Manager
- Configuración de Virtual Deliverability Manager

Introducción a Virtual Deliverability Manager

Para empezar a utilizar Virtual Deliverability Manager con la cuenta, debe habilitarlo mediante el asistente de incorporación de la consola de Amazon SES, con el que configurará el seguimiento de las interacciones y la entrega compartida optimizada. Virtual Deliverability Manager utiliza el seguimiento de las interacciones y la entrega compartida optimizada para supervisar los envíos y ayudarle a mejorar su capacidad de entrega y reputación.

- Seguimiento de las interacciones: la capacidad de supervisar el comportamiento de interacción de los destinatarios mediante eventos de apertura y clic utilizando un píxel de seguimiento dentro de un enlace encapsulado. Cuando se activa, el píxel de seguimiento proporciona una marca temporal de cuándo se abrió un mensaje e indica en qué enlaces hizo clic el destinatario. Al activar esta opción, las URL y los enlaces se modifican para incluir los encapsuladores de seguimiento de las interacciones de Amazon SES.

- Entrega compartida optimizada: elige automáticamente la IP óptima que se utilizará al enviar correos electrónicos, lo que mejora la entrega final de los mensajes a los destinatarios. Esto no se aplica a las direcciones IP dedicadas.

Si bien el seguimiento de las interacciones y la entrega compartida optimizada están activados de forma predeterminada en el asistente de incorporación, tiene la opción de desactivarlos. Le recomendamos encarecidamente que mantenga ambas características habilitadas para aprovechar al máximo el administrador virtual de entrega.

Empezar a utilizar Virtual Deliverability Manager con la consola de Amazon SES

El siguiente procedimiento muestra cómo empezar a utilizar Virtual Deliverability Manager con la consola de Amazon SES.

Para empezar a trabajar con Virtual Deliverability Manager con la consola de Amazon SES

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación izquierdo, elija Virtual Delivery Manager.
3. Elija cualquiera de los botones de Get started with Virtual Deliverability Manager (Introducción a Virtual Deliverability Manager) en la página Virtual Deliverability Manager overview (Información general de Virtual Deliverability Manager).
4. En la página Select Engagement tracking (Seleccionar Seguimiento de las interacciones), acepte el valor predeterminado o elija Turn off engagement tracking (Desactivar el seguimiento de las interacciones) y, a continuación, elija Next (Siguiente).

   > **Note**
   >
   > Activar el seguimiento de las interacciones modifica las URL y los enlaces para incluir los encapsuladores de seguimiento de las interacciones de Amazon SES.

5. En la página Select Optimized shared delivery (Seleccionar Entrega compartida optimizada), acepte la opción predeterminada o elija Turn off optimized shared delivery (Desactivar la entrega compartida optimizada) y, a continuación, elija Next (Siguiente).

> **Important**
>
> Es posible que la entrega compartida optimizada provoque retrasos preventivos en el envío de los correos electrónicos a fin de proteger su reputación como remitente. Si tiene una carga de trabajo crítica que se debe enviar sin retraso, le recomendamos que no habilite esta configuración. En su lugar, utilice conjuntos de configuración para el envío y solo habilite la entrega compartida optimizada para aquellos conjuntos de configuración en los que se puedan permitir retrasos.

6. Revise las opciones para el seguimiento de las interacciones y la entrega compartida optimizada en la página Review and enable (Revisar y habilitar). Elija Previous (Anterior) si desea volver atrás y realizar cambios; de lo contrario, elija Enable Virtual Deliverability Manager (Habilitar Virtual Deliverability Manager).

   Se abrirá la página Virtual Deliverability Manager settings (Configuración de Virtual Deliverability Manager). El panel Subscription overview (Información general de la suscripción) indica el estado de Virtual Deliverability Manager y el panel Additional settings (Configuración adicional) indica el estado de Engagement tracking (Seguimiento de las interacciones) y Optimized shared delivery (Entrega compartida optimizada).

Una vez que haya activado Virtual Deliverability Manager para la cuenta, puede definir ajustes personalizados sobre cómo un conjunto de configuración utilizará el seguimiento de las interacciones y la entrega compartida optimizada invalidando la forma en que se han definido en Virtual Deliverability Manager. Esto le confiere flexibilidad para personalizar el envío de correos electrónicos para campañas de correo electrónico específicas. Por ejemplo, puede habilitar el seguimiento de las interacciones y la entrega compartida optimizada para los correos electrónicos de marketing y desactivarlos para los correos electrónicos transaccionales. Consulte las opciones de Virtual Deliverability Manager al crear o editar un conjunto de configuración.

Empezar a utilizar Virtual Deliverability Manager con la AWS CLI

En los siguientes ejemplos se muestra cómo empezar a utilizar Virtual Deliverability Manager con la AWS CLI.

Para empezar a trabajar con Virtual Deliverability Manager con la AWS CLI

Puede utilizar la operación `PutAccountVdmAttributes` en la API v2 de Amazon SES para comenzar a utilizar Virtual Deliverability Manager. Puede llamar a esta operación desde la AWS CLI, como se muestra en los siguientes ejemplos.

- Habilite Virtual Deliverability Manager en la cuenta:

```
aws --region us-east-1 sesv2 put-account-vdm-attributes --vdm-attributes
 VdmEnabled=ENABLED
```

- Habilite el seguimiento de las interacciones y la entrega compartida optimizada mediante un archivo de entrada:

```
aws --region us-east-1 sesv2 put-account-vdm-attributes --cli-input-json file://
attributes.json
```

  El archivo de entrada tiene este aspecto:

```
{
    "VdmAttributes": {
        "VdmEnabled": "ENABLED",
        "DashboardAttributes": {
            "EngagementMetrics": "ENABLED"
        },
        "GuardianAttributes": {
            "OptimizedSharedDelivery": "ENABLED"
        }
    }
}
```

  Los valores de los parámetros y los tipos de datos relacionados se pueden encontrar en el tipo de datos `VdmAttributes` de la referencia de la API v2 de Amazon SES.

> **Note**
>
> Al activar el seguimiento de las interacciones, las URL y los enlaces se modifican para incluir los encapsuladores de seguimiento de las interacciones de Amazon SES.

> **Important**
>
> Es posible que la entrega compartida optimizada provoque retrasos preventivos en el envío de los correos electrónicos a fin de proteger su reputación como remitente. Si tiene una carga de trabajo crítica que se debe enviar sin retraso, le recomendamos que no habilite esta configuración. En su lugar, utilice conjuntos de configuración para el envío y solo habilite la entrega compartida optimizada para aquellos conjuntos de configuración en los que se puedan permitir retrasos.

- Para verificar el resultado:

```
aws --region us-east-1 sesv2 get-account
```

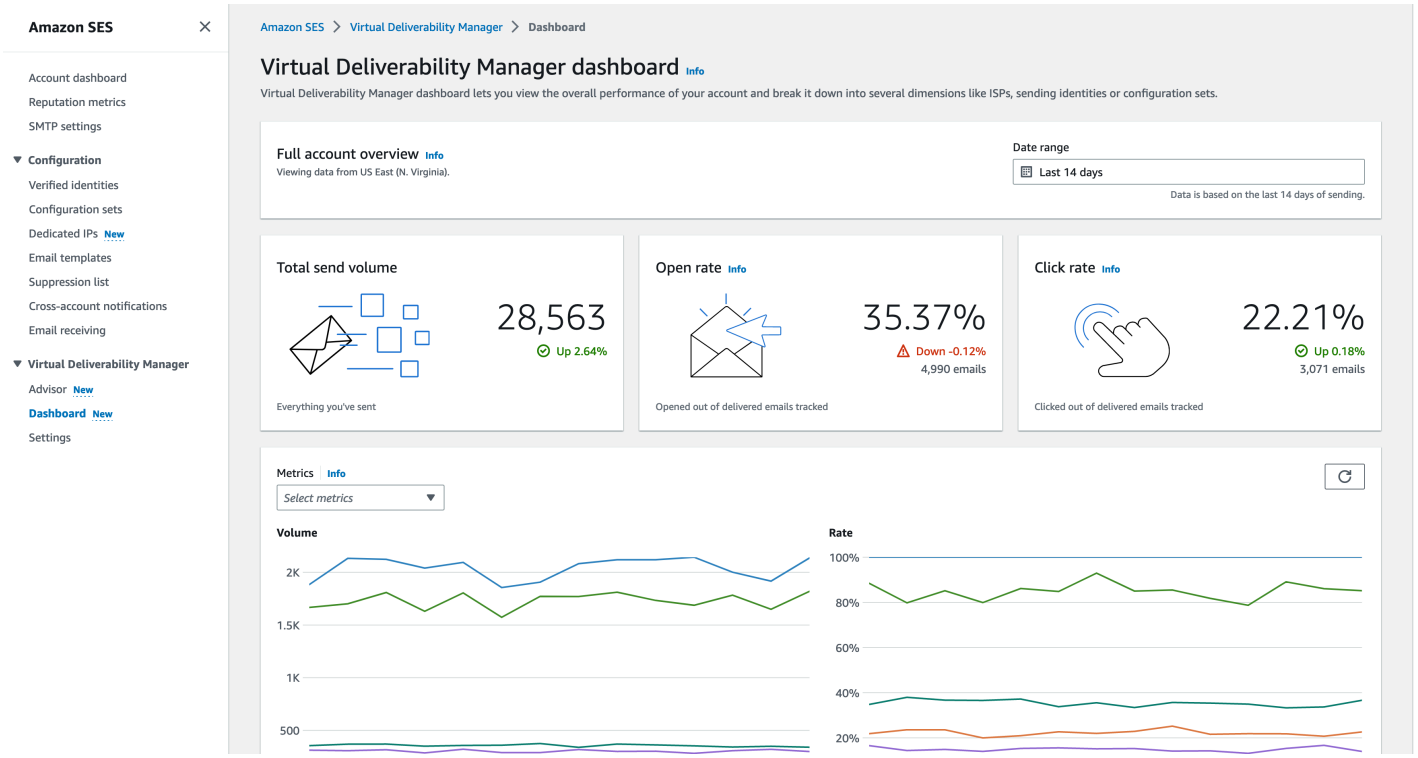
- Para definir ajustes personalizados sobre la forma en que un conjunto de configuración utilizará el seguimiento de las interacciones y la entrega compartida optimizada invalidando la forma en que se han definido en Virtual Deliverability Manager, consulte el ejemplo de la AWS CLI en the section called “Configuración”.

Panel Virtual Deliverability Manager

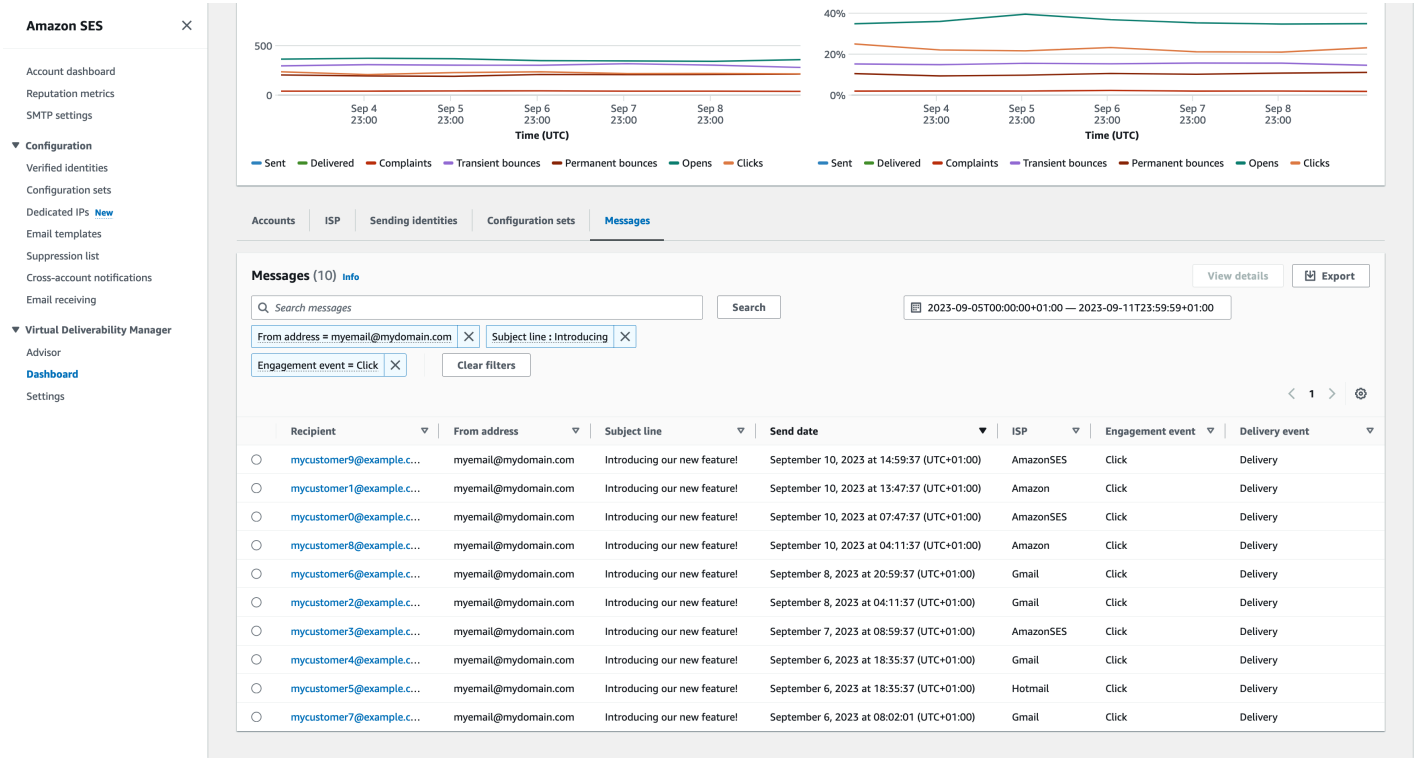
El panel ofrece vistas de alto nivel del programa de capacidad de entrega de la cuenta, como tarjetas fáciles de leer y gráficos de series temporales que muestran la capacidad de entrega y la reputación a través de las tasas de apertura o clics y de entrega y las estadísticas de devoluciones o reclamaciones. El panel también ofrece una vista más detallada, lo que le permite acceder a datos de tablas específicos más detallados cuando haya un problema relacionado con un ISP, una identidad de envío o un conjunto de configuración determinados que esté asociado a una campaña de correo electrónico.

Poder ver las cosas desde un nivel general alto con la capacidad de ver también los detalles específicos le permite centrarse en las áreas problemáticas de la capacidad de entrega en lugar de tener que revisar el programa de correo electrónico en su conjunto. Este nivel de información también le permite detectar tendencias y posibles problemas antes de que se conviertan en problemas de capacidad de entrega mayores, como aplazamientos o bloqueos.

La información general de una cuenta en el panel del administrador virtual de entrega que muestra las tarjetas y los gráficos de series temporales.



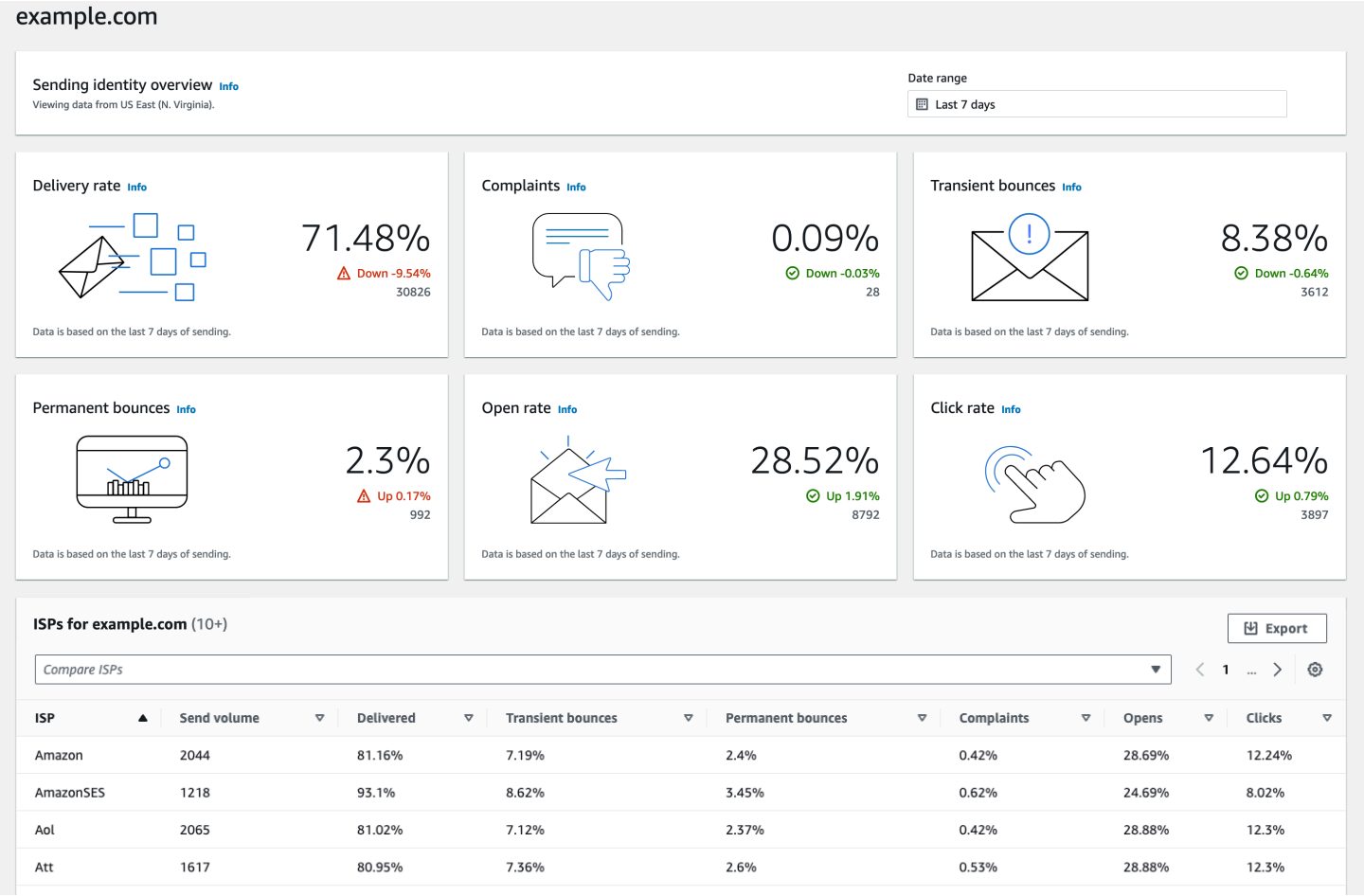
La tabla Mensajes seleccionada en el panel del Administrador virtual de entrega muestra los mensajes enviados que coinciden con el intervalo de fechas y los criterios de filtrado.



Los datos detallados que proporciona el panel pueden ayudarle a mejorar la reputación como remitente y a calcular las fechas y horas ideales para aumentar las interacciones y las conversiones del programa de correo electrónico, con la posibilidad de desglosar conjuntos de datos específicos:

- Datos del ISP: valiosos cuando tiene un problema de capacidad de entrega a un ISP o proveedor de buzones específico. En lugar de intentar ajustar toda la cuenta, lo que de otro modo podría funcionar bien, se puede centrar en el punto de conexión problemático y seguir las prácticas recomendadas para mejorar la reputación del remitente para ese ISP y restaurar la buena capacidad de entrega de la bandeja de entrada para llegar a los destinatarios. También es importante entender la distribución de ISP, ya que puede enviar mayor peso a un ISP o proveedor de bandeja de correo que a otros. Debe asegurarse de que los destinatarios finales siempre proporcionen tráfico e interactúen para tener un impacto positivo en la conversión del correo electrónico.
- Envío de datos de conjuntos de identidad y configuración: útil para ayudarle a identificar las identidades de envío y los conjuntos de configuración que contribuyen al problema general de capacidad de entrega de la cuenta. Se puede centrar en ellos específicamente, ajustar las configuraciones y, posiblemente, reducir el envío con una identidad determinada hasta que se resuelva el problema. Por ejemplo, una identidad de envío enviada accidentalmente a una lista de supresión, da lugar a que todo el tráfico pase por esa identidad. Esa identidad está asociada a un conjunto de configuración, lo que provoca problemas de capacidad de entrega. En estos casos, resulta útil poder identificar la identidad de envío o el conjunto de configuración para poder centrarse en corregir ese problema específicamente, en lugar de analizar toda la cuenta para tratar de identificar la causa principal del problema de capacidad de entrega.

Los datos detallados se muestran en el panel del Administrador virtual de entrega para la identidad de envío seleccionada, example.com: las tarjetas muestran las métricas de capacidad de entrega y reputación. La tabla muestra todos los ISP a los que la identidad remitente envió correo con tasas de métricas para cada ISP dentro del intervalo de fechas ingresado.



Uso del panel Virtual Deliverability Manager en la consola de Amazon SES

El siguiente procedimiento muestra cómo utilizar el panel Virtual Deliverability Manager de la consola de Amazon SES para ver las estadísticas generales de capacidad de entrega y reputación y analizar las áreas problemáticas.

Para usar el panel Virtual Deliverability Manager para ver datos de nivel alto y más detallados de las métricas de capacidad de entrega de la cuenta

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. En el panel de navegación izquierdo, elija Dashboard (Panel) en Virtual Deliverability Manager.

> **Note**
>
> El Dashboard (Panel) no estará visible si no ha habilitado Virtual Deliverability Manager para la cuenta. Para obtener más información, consulte the section called “Introducción”.

3. En el panel Información general de la cuenta completa, elija un intervalo de fechas que se utilizará para todas las métricas de las tarjetas, los gráficos de series temporales y las tablas detalladas.

   - En el campo Date range (Intervalo de fechas), elija Relative range (Intervalo relativo) (predeterminado) o Absolute range (Intervalo absoluto).

     - Relative range (Intervalo relativo): seleccione el botón de opción que corresponda al número de días deseado.
       - Intervalo personalizado: ingrese un intervalo en días (hasta 60), semanas (hasta 8) o meses (hasta 2).
     - Intervalo absoluto: la primera fecha que elija será la Fecha de inicio, la segunda fecha será la Fecha de finalización, sin superar los 60 días en total. Para especificar un solo día, elíjalo para la fecha de Start (Inicio) y para la End date (Fecha de finalización).

   > **Note**
   >
   > Lo siguiente se aplica a todos los intervalos de fechas del panel:
   >
   > - Todas las fechas y horas son UTC.
   > - Para las fechas de Relative range (Intervalo relativo), el último día termina en su marca temporal de medianoche de UTC. Por ejemplo, si elige Last 7 days (Últimos 7 días), el séptimo día sería ayer y finalizaría a medianoche.
   > - Si el intervalo de fechas es superior a 30 días, la columna % de diferencia de la tabla de estadísticas de la cuenta y los porcentajes de cambio de las tarjetas no tendrán ningún valor (indicado mediante un guión -).

4. Las tarjetas, los gráficos de series temporales y todas las tablas detalladas, las estadísticas de cuentas, el ISP, las identidades de envío y los conjuntos de configuración muestran los totales de las métricas calculados a partir del intervalo de fechas ingresado y utilizan la matemática métrica descrita en Cómo se calculan las métricas del panel.

- Para crear un archivo local `.csv` de los datos que está viendo actualmente en la tabla ISP, identidades de envío o conjuntos de configuración, seleccione el botón Exportar.

5. Los gráficos de series temporales que realizan la progresión del Volumen y la Velocidad para el intervalo de fechas que ha ingresado se muestran en el panel Métricas. Al pasar el ratón sobre un intervalo de fechas en los gráficos, se mostrará el número de volúmenes exacto o el porcentaje de la frecuencia en función de una agregación diaria. Puede filtrar las métricas que desea ver mediante el menú desplegable Seleccionar métricas.
6. Elija la pestaña Accounts (Cuentas) para mostrar la tabla de Accounts statistics (Estadísticas de cuentas).

   - Esta tabla ofrece información general de las métricas de capacidad de entrega y reputación y muestra el Volume (Volumen) total, % Rate (Tasa de %) y % Difference (Diferencia de %) para Sent (Enviados), Delivered (Entregados), Complaints (Reclamaciones), Transient & Permanent bounces (Devoluciones transitorias y permanentes), Opens & Clicks (Aperturas y clics) según lo calculado a partir del intervalo de fechas ingresado.

   > **Note**
   >
   > Si el intervalo de fechas es superior a 30 días, la columna % de diferencia no tendrá ningún valor (indicado mediante un guión `-`).

7. Elija la pestaña ISP para mostrar la tabla de ISP.

   - Esta tabla muestra las métricas para Send volume (Volumen de envíos), Delivered (Entregados), Transient & Permanent bounces (Devoluciones transitorias y permanentes), Complaints (Reclamaciones), Opens & Clicks (Aperturas y clics) de cada ISP que ha enviado, calculadas a partir del intervalo de fechas ingresado.
   - Para filtrar ISP específicos, dentro del cuadro de búsqueda Comparar ISP, elija la casilla de verificación correspondiente para cada ISP que desee incluir.
   - Para crear un archivo `.csv` local de los datos que está viendo actualmente en esta tabla, seleccione el botón Exportar.

8. Elija la pestaña Sending identities (Identidades de envío) para mostrar la tabla de Sending identities (Identidades de envío).

   - Esta tabla muestra las métricas para Send volume (Volumen de envío), Delivered (Entregados), Transient & Permanent bounces (Devoluciones transitorias y permanentes),

Complaints (Reclamaciones), Opens & Clicks (Aperturas y clics) de cada identidad de envío que ha usado, calculadas a partir del intervalo de fechas ingresado.

- Para filtrar identidades de envío específicas, dentro del cuadro de búsqueda Comparar identidades, elija la casilla de verificación correspondiente para cada identidad que desee incluir.
- Para obtener información detallada sobre una identidad de envío específica, elija su nombre en la columna Sending identity (Identidad de envío).
  - Aparecerán tarjetas con la Tasa de entrega, las Reclamaciones, las Devoluciones transitorias y permanentes, las Tasas de aperturas y clics para la identidad de envío seleccionada, calculadas a partir del intervalo de fechas ingresado.
  - Los gráficos de series temporales se actualizarán y mostrarán todas las métricas de la identidad de envío seleccionada calculadas a partir del intervalo de fechas ingresado.
  - Se mostrará una tabla de ISP con todos los ISP a los que la identidad remitente envió correo con las métricas proporcionadas para cada ISP calculadas a partir del intervalo de fechas ingresado.
- Para crear un archivo `.csv` local de los datos que está viendo actualmente en esta tabla, seleccione el botón Exportar.

9. Elija la pestaña Configuration sets (Conjuntos de configuración) para mostrar la tabla Configuration sets (Conjuntos de configuración).

   - Esta tabla muestra las métricas para Send volume (Volumen de envío), Delivered (Entregados), Transient & Permanent bounces (Devoluciones transitorias y permanentes), Complaints (Reclamaciones), Opens & Clicks (Aperturas y clics) de cada conjunto de configuración que ha usado para enviar correos, calculadas a partir del intervalo de fechas ingresado.
   - Para filtrar conjuntos de configuración específicos, dentro del cuadro de búsqueda Comparar conjuntos de configuración, elija la casilla de verificación correspondiente para cada conjunto de configuración que desee incluir.
   - Para profundizar en un conjunto de configuración específico, elija su nombre en la columna Configuration set (Conjunto de configuración).
     - Aparecerán tarjetas con la Tasa de entrega, las Reclamaciones, las Devoluciones transitorias y permanentes, las Tasas de aperturas y clics para el conjunto de configuración seleccionado, calculadas a partir del intervalo de fechas ingresado.

- Los gráficos de series temporales se actualizarán y mostrarán todas las métricas del conjunto de configuración seleccionado, calculadas a partir del intervalo de fechas ingresado.
- Se mostrará una tabla de ISP con una lista de todos los ISP en los que se utilizó el conjunto de configuración para enviar correo con las métricas proporcionadas para cada ISP, calculadas a partir del intervalo de fechas ingresado.

- Para crear un archivo `.csv` local de los datos que está viendo actualmente en esta tabla, seleccione el botón Exportar.

10. Elija la pestaña Mensajes para mostrar la tabla Mensajes.

    Se trata de una tabla interactiva que le permite buscar y encontrar los mensajes enviados. Para cada mensaje, puede realizar un seguimiento de su estado actual de entrega e interacción, del historial de eventos y ver la respuesta devuelta por el proveedor del buzón. En los puntos siguientes se describen las formas de buscar determinados mensajes:

    - Si selecciona dentro del selector de intervalo de fechas, podrá filtrar los mensajes que haya enviado en los últimos 30 días. Si no selecciona un intervalo de fechas, su búsqueda se realizará de forma predeterminada en los últimos 7 días, incluido el día actual, en su zona horaria.
    - En el campo Buscar mensajes puede filtrar por Destinatario, Dirección del remitente, Línea de asunto, ISP, Evento de participación, Evento de entrega e ID de mensaje. Se aplican las propiedades siguientes:
        - En función del tipo de filtro, introduzca una cadena de texto que distinga entre mayúsculas y minúsculas o seleccione un valor de una lista.
        - Evento de participación está limitado a un único valor, Línea de asunto puede tener hasta dos valores y todos los demás filtros pueden tener hasta cinco valores por búsqueda. El filtrado por ID de mensaje excluirá cualquier otro filtro que haya seleccionado, incluido el intervalo de fechas.
        - La columna ID de mensaje está oculta de forma predeterminada, pero puede mostrarse si se selecciona el icono de engranaje para personalizar la forma de ver la tabla Mensajes.
    - Una vez elegidos los filtros y el intervalo de fechas, elija Buscar y la tabla se completará con los mensajes que coincidan con sus criterios de búsqueda. La tabla puede cargar hasta 100 mensajes. Si la búsqueda arroja más de 100 mensajes, los 100 mensajes de la tabla son un ejemplo aleatorio del total devuelto.

- Al seleccionar el botón de opción de un mensaje seguido de la selección de Ver detalles, aparecerá una barra lateral de Información del mensaje que contiene detalles del historial completo de eventos del mensaje, el más reciente en la parte superior, y cualquier respuesta o código de diagnóstico devuelto por el proveedor del buzón.
- Para crear un archivo `.csv` local de los datos que está viendo actualmente en esta tabla, seleccione el botón Exportar.

Acceso a los datos de las métricas de Virtual Deliverability Manager mediante la AWS CLI

En los siguientes ejemplos se muestra cómo acceder a los datos de métricas de Virtual Deliverability Manager con la AWS CLI. Son los mismos datos usados en el panel Virtual Deliverability Manager en la consola.

Para acceder a los datos de las métricas de capacidad de entrega mediante el AWS CLI

Puede utilizar la operación `BatchGetMetricData` en la API v2 de Amazon SES para acceder a los datos de métricas de capacidad de entrega. Puede llamar a esta operación desde la AWS CLI , como se muestra en los siguientes ejemplos.

- Acceda a los datos de las métricas de capacidad de entrega:

```
aws --region us-east-1 sesv2 batch-get-metric-data --cli-input-json file://sends.json
```

- El archivo de entrada tiene este aspecto:

```
{
 "Queries": [
   {
     "Id": "Retrieve-Account-Sends",
     "Namespace": "VDM",
     "Metric": "SEND",
     "StartDate": "2022-11-04T00:00:00",
     "EndDate": "2022-11-05T00:00:00"
    }
 ]
}
```

Más información sobre los valores de los parámetros y los tipos de datos relacionados se pueden encontrar enlazando el tipo de datos `BatchGetMetricDataQuery` de la referencia de la API v2 de Amazon SES.

Filtrar y exportar los datos de las métricas de capacidad de entrega mediante AWS CLI

Este ejemplo le muestra cómo utilizar la operación `CreateExportJob` para filtrar y exportar sus datos de métricas de capacidad de entrega a un archivo .csv o .json mediante la AWS CLI. Se trata de los mismos datos utilizados en las tablas ISP, Identidades de envío y Conjuntos de configuración del panel del Administrador virtual de entrega.

Para filtrar y exportar los datos de las métricas de capacidad de entrega a un archivo.csv o .json mediante AWS CLI

Puede utilizar la operación `CreateExportJob` junto con el tipo de datos `MetricsDataSource` en la API v2 de Amazon SES para filtrar y exportar sus datos de métrica a un archivo .csv o .json. Puede llamar a esta operación desde la siguiente, AWS CLI como se muestra en el siguiente ejemplo.

- Filtrar y exportar sus datos de métricas de capacidad de entrega mediante un archivo de entrada:

```
aws --region us-east-1 sesv2 create-export-job --cli-input-json file://metric-export-input.json
```

- En este ejemplo, el archivo de entrada utiliza parámetros `MetricsDataSource` para filtrar todos los ISP a los que ha enviado correo (se muestra el porcentaje de entregas correctas en el intervalo de fechas dado) y un formato .csv especificado para el archivo de salida:

```
{
    "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"
    }
}
```

Puede encontrar más información sobre los valores de los parámetros y los tipos de datos relacionados en `MetricsDataSource` como un objeto del tipo `ExportDataSource` en la referencia de la API v2 de Amazon SES.

Encuentra los mensajes enviados, su estado de entrega e interacción y exporta los resultados mediante el AWS CLI

Estos ejemplos le muestran cómo utilizar la operación `CreateExportJob` para buscar y encontrar mensajes concretos que haya enviado, ver su estado actual de entrega e interacción, y exportar los resultados de su búsqueda a un archivo .csv o .json mediante la AWS CLI. Son los mismos datos que se utilizan en la tabla Mensajes del panel del Administrador virtual de entrega.

Para buscar los mensajes enviados, su estado de entrega e interacción, y exportar los resultados a un archivo.csv o .json mediante el AWS CLI

Puede utilizar la operación `CreateExportJob` junto con el tipo de datos `MessageInsightsDataSource` en la API v2 de Amazon SES para aplicar filtros con el fin de encontrar mensajes concretos que haya enviado, ver su estado de entrega e interacción, y exportar los resultados a un archivo .csv o .json. Puede llamar a esta operación de la siguiente manera AWS CLI , tal como se muestra en los siguientes ejemplos.

> **Note**
>
> Si la búsqueda filtrada arroja más de 10 000 mensajes, los 10 000 mensajes del conjunto de resultados de la API son un ejemplo aleatorio del total devuelto.

- Buscar mensajes enviados, ver su estado actual y exportar los resultados mediante un archivo de entrada:

```
aws --region us-east-1 sesv2 create-export-job --cli-input-json file://message-insights-export-input.json
```

- En este ejemplo, el archivo de entrada utiliza parámetros `MessageInsightsDataSource` para filtrar por un asunto igual a “¡Las rebajas terminan esta noche!” y un formato .csv especificado para el archivo de salida:

```
{
    "ExportDataSource": {
        "MessageInsightsDataSource": {
            "StartDate": "2023-07-01T00:00:00",
            "EndDate": "2023-07-10T00:00:00",
            "Include": {
                "Subject": [
                    "Sale Ends Tonight!"
                ]
            }
        }
    },
    "ExportDestination": {
        "DataFormat": "CSV"
    }
}
```

- En este ejemplo, el archivo de entrada utiliza `MessageInsightsDataSource`parámetros para filtrar por un asunto que comienza por «Hola», se envía con una « FromEmailAddress información» a los destinos que terminan en «@example .com» y un formato.json especificado para el archivo de salida:

```
{
    "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"
    }
}
```

- En este ejemplo, el archivo de entrada utiliza `MessageInsightsDataSource`parámetros para filtrar por un asunto que comienza por «Hola», excluir los resultados que tienen "noreply@example.com" como letra "" y especificar el formato.csv para el archivo de salida: FromEmailAddress

```
{
    "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"
    }
}
```

- En este ejemplo, el archivo de entrada utiliza `MessageInsightsDataSource`parámetros para filtrar por un asunto que comienza por «Hola», se envía con una «información» a destinos FromEmailAddress que terminan en «@example .com», se utiliza Gmail como ISP, un último evento de entrega es «DELIVERY», un último evento de participación que es «OPEN» o «CLICK» y un formato.json especificado para el archivo de salida:

```
{
    "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"
    }
}
```

- En este ejemplo, el archivo de entrada utiliza `MessageInsightsDataSource`parámetros para filtrar los destinos que terminan en «@example1 .com», «@example2 .com» o

«@example3 .com», excluir los mensajes con un LastDeliveryEvent valor igual a «SEND» o «DELIVERY» y un formato .csv especificado para el archivo de salida:

```
{
    "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"
    }
}
```

Puede encontrar más información sobre los valores de los parámetros y los tipos de datos relacionados en `MessageInsightsDataSource` como un objeto del tipo `ExportDataSource` en la referencia de la API v2 de Amazon SES.

Administración de sus trabajos de exportación mediante la AWS CLI

En estos ejemplos se describe cómo administrar sus trabajos de exportación enumerándolos, obteniendo información sobre ellos y cancelándolos mediante la AWS CLI.

Para ver una lista de tus trabajos de exportación, usa el AWS CLI

Puede utilizar la operación `ListExportJobs` en la API v2 de Amazon SES para enumerar los trabajos de exportación. Puede llamar a esta operación desde el AWS CLI , como se muestra en los siguientes ejemplos.

- Enumerar los trabajos de exportación:

```
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
```

- El archivo de entrada tiene este aspecto:

```
{
  "NextToken": "",
  "PageSize": 0,
  "ExportSourceType": "METRICS_DATA",
  "JobStatus": "CREATED"
}
```

  Encontrará más información sobre los valores de los parámetros de la operación `ListExportJobs` en la referencia de la API v2 de Amazon SES.

Para obtener información sobre su trabajo de exportación, utilice el AWS CLI

Puede utilizar la operación `GetExportJob` de la API v2 de Amazon SES para obtener información sobre su trabajo de exportación. Puede llamar a esta operación desde el, tal y AWS CLI como se muestra en los ejemplos siguientes.

- Obtener información sobre el trabajo de exportación:

```
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
```

- El archivo de entrada tiene este aspecto:

```
{
    "JobId": "e2220d6b-dce5-45f2-bf60-3287a465b732"
}
```

Encontrará más información sobre los valores de los parámetros de la operación `GetExportJob` en la referencia de la API v2 de Amazon SES.

Para cancelar el trabajo de exportación mediante el AWS CLI

Puede utilizar la operación `CancelExportJob` en la API v2 de Amazon SES para cancelar el trabajo de exportación. Puede llamar a esta operación desde el AWS CLI , como se muestra en los siguientes ejemplos.

- Cancelar el trabajo de exportación:

```
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
```

- El archivo de entrada tiene este aspecto:

```
{
    "JobId": "e2220d6b-dce5-45f2-bf60-3287a465b732"
}
```

Encontrará más información sobre los valores de los parámetros de la operación `CancelExportJob` en la referencia de la API v2 de Amazon SES.

Ver el historial completo de eventos de un mensaje y las respuestas del ISP mediante el AWS CLI

En el siguiente ejemplo se describe cómo ver los detalles del historial completo de eventos de un mensaje y cualquier respuesta o código de diagnóstico devuelto por el proveedor de buzones mediante la AWS CLI. Son los mismos datos que se utilizan en la barra lateral Información de

mensaje tras seleccionar el botón de opción de un mensaje en la tabla Mensajes del panel del Administrador virtual de entrega.

Para ver el historial de eventos de un mensaje y las respuestas del ISP mediante el AWS CLI

Puede utilizar la operación `GetMessageInsights` en la API v2 de Amazon SES para ver los detalles de un mensaje enviado. Puede llamar a esta operación desde, AWS CLI como se muestra en el siguiente ejemplo.

- Consultar los detalles del mensaje de un correo electrónico enviado identificado por su identificador de mensaje:

  ```
  aws --region us-east-1 sesv2 get-message-insights --message-id
   01000100001000dd-2a19190d-99d4-0000-9f00-deb5bbf2bfbe-000001
  ```

  Encontrará más información sobre los valores de los parámetros de la operación `GetMessageInsights` en la referencia de la API v2 de Amazon SES.

Cómo se calculan las métricas del panel Virtual Deliverability Manager

Todas las tasas de tarjetas y tablas detalladas que se muestran en el panel del Administrador virtual de entrega calculan las métricas para el intervalo de fechas escrito en el panel Información general de la cuenta completa.

Los porcentajes de tasas de las métricas que se muestran en el panel se calculan como se describe en la tabla. Las cuatro últimas columnas representan los calificadores de las matemáticas básicas que se utilizan para derivar las métricas mostradas. Por ejemplo, la Open rate (Tasa de apertura) se calcula dividiendo el total abierto por el total entregado en el caso de los mensajes HTML que se entregan con el seguimiento de las interacciones activado. No reflejan ninguno de los mensajes que envió sin el seguimiento de las interacciones y no están codificados en HTML.

% de tasa	Cómo se calcula	Con el seguimiento de las interacciones habilitado y HTML	Y con al menos 1 enlace rastreado	Entregado a los ISP con un FBL de SES	Se excluye si se encuentra en la lista de supresión al nivel de la cuenta
Open rate (Tasa de apertura)	total abierto/total entregado	✗			
Tasa de clics	total de clics/total entregado	✗	✗		
Complaint rate (Tasa de reclamaciones)	total de reclamaciones/total entregado			✗	✗
Porcentaje de entregas	total entregado/total enviado				
Tasa de devoluciones transitorias	total de devoluciones transitorias/total enviado				✗
Tasa de devoluciones permanente	total de devoluciones permanentes/total enviado				✗
Volumen de envíos total	No se muestra el % de la tasa (todo lo que ha enviado; siempre al 100 %)				

Cómo se calculan la tasa de diferencia y los totales de volumen para todas las métricas:

- % de diferencia: diferencia en el total de métricas en comparación con el total de métricas anterior para el intervalo de fechas dado. Por ejemplo, si los últimos 7 días son el intervalo de fechas especificado, la Tasa métricas de los últimos 7 días: tasa de métricas de los 7 días anteriores.

- El % de diferencia para el volumen total de envíos se calcula de forma diferente. Por ejemplo, (Volumen de envío de los últimos 7 días: volumen de envío de los 7 últimos días)/Volumen de envío de los últimos 7 días.

- Volumen: recuento total de cada métrica.

> **Note**
>
> - La columna Delivered (Entregados) de las tablas desglosadas muestra el volumen entregado directamente sin los calificadores de entrega que se utilizan para calcular las tasas de apertura, clics y reclamaciones.
> - Virtual Deliverability Manager solo realiza un seguimiento de las métricas de los correos electrónicos que tienen un destinatario; los correos con varios destinatarios no se cuentan en ninguna de las métricas del panel Virtual Deliverability Manager.
>   - En estos casos, los recuentos de métricas de Virtual Deliverability Manager serán inferiores a los recuentos de CloudWatch métricas de Amazon, ya que CloudWatch las métricas incluyen correos electrónicos con varios destinatarios.
> - Los correos electrónicos enviados al simulador de bandeja de correo de SES no se cuentan en ninguna de las métricas del panel Virtual Deliverability Manager.
> - Los correos electrónicos enviados a través de la cuenta de un remitente delegado (anteriormente, el envío entre cuentas) no se cuentan en ninguna de las métricas del panel del Administrador virtual de entrega.

> **Important**
>
> La protección de la privacidad de Apple Mail y su impacto en las tasas de interacción: como resultado de que Apple implementara su función de protección de la privacidad del correo (MPP) para los dispositivos Apple a partir de iOS15, las cifras de interacción se han exagerado, ya que el MPP activa la apertura cuando se inicia la aplicación Apple Mail, no necesariamente cuando el destinatario abre o hace clic en un mensaje. Esto hace que los datos de interacción parezcan mucho más altos de lo que normalmente serían y esto es algo que los especialistas en marketing por correo electrónico deberán tener en cuenta al revisar la interacción. Hay otras formas de identificar la interacción, como la actividad web, el uso de aplicaciones o portales y también el uso de datos proxy de dispositivos que no son de Apple para crear una métrica agregada. Lo importante es centrarse en las tendencias de

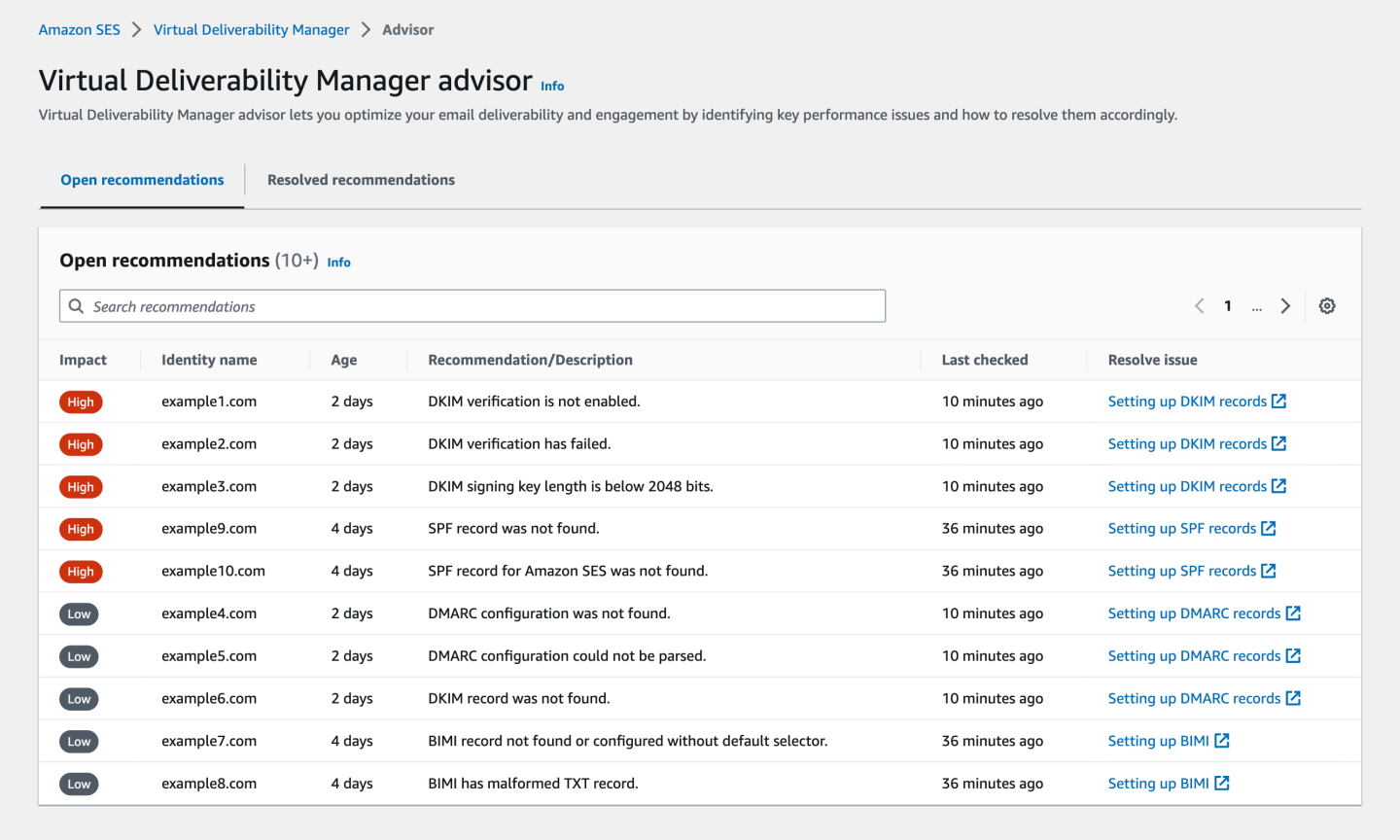
interacción, ya que pueden indicar si hay algún problema con el envío del correo electrónico. Para obtener más información, consulte protección de la privacidad de correo electrónico de Apple.

Asesor de Virtual Deliverability Manager

El asesor de Virtual Deliverability Manager le ayuda a optimizar la capacidad de entrega y las interacciones de correo electrónico al identificar los problemas clave de rendimiento e infraestructura en la cuenta y enviar los niveles de identidad que están afectando negativamente a su capacidad de entrega de correo electrónico y su reputación. Ofrece soluciones proporcionando directrices específicas para resolver el problema identificado.

Las recomendaciones de infraestructura del asesor se muestran en la tabla Open recommendations (Recomendaciones abiertas). Las recomendaciones identifican los problemas de autenticación del correo electrónico estándar, como los casos en los que los registros SPF, DKIM, DMARC o BIMI no existen o tienen problemas con la configuración, como un formato incorrecto o una longitud de clave demasiado corta. Se clasifican según la gravedad del Impact (Impacto), el Identity name (Nombre de la identidad) del dominio de envío y la Age (Antigüedad) de la alerta. En la barra de búsqueda, un cuadro de lista ofrece la opción de filtrar por nivel de impacto, categoría de infraestructura o nombre de la identidad de envío. La columna Last checked (Última comprobación) muestra la hora relativa a la que se actualizó la recomendación por última vez, como «Justo ahora» o «Hace 15 minutos». La última columna, Resolve issue (Resolver problema), proporciona un enlace a la sección correspondiente de la Guía para desarrolladores de Amazon SES con instrucciones para resolver el problema identificado.

Las recomendaciones abiertas se muestran en el asesor de Virtual Deliverability Manager ordenadas por nivel de impacto.



Si no tiene ninguna notificación del asesor en curso, un mensaje indicará que no tiene ninguna recomendación abierta. Le recomendamos que compruebe el asesor de forma periódica. Si lo desea, puede integrar estos eventos de notificación de asesores con Amazon EventBridge para crear aplicaciones escalables basadas en eventos, como se explica en. Monitorización mediante EventBridge

También puede acceder a la tabla Resolved recommendations (Recomendaciones resueltas) desde la página del asesor de Virtual Deliverability Manager, en la que se muestran los problemas de infraestructura que ha resuelto siguiendo las directrices del asesor. Las recomendaciones resueltas se muestran con un estado inicial que describe el problema antes de que se resolviera. Las recomendaciones resueltas caducan a los 30 días.

¿Qué busca el asesor de Virtual Entregability Manager

En la sección anterior, explicamos que el asesor de Virtual Deliverability Manager comprueba su dominio de envío para determinar si ha configurado una infraestructura autenticada de forma segura, a fin de garantizar que mantiene una alta tasa de capacidad de entrega del correo electrónico y una buena reputación como remitente. Antes de activar el asesor de Virtual Deliverability Manager,

creemos que sería útil que supiera exactamente qué es lo que comprueba el asesor y qué es lo que busca en esas comprobaciones.

Puede utilizar esta tabla como referencia para revisar la configuración de su dominio de envío y corregir cualquiera de estos elementos que no se ajusten a los estándares enumerados en esta tabla antes de que se conviertan en problemas de los que el asesor tenga que avisarle.

Tipo de verificación	Mensaje del asesor	¿Por qué te alerta el asesor	Más información
Configuración DKIM	La verificación DKIM no está habilitada.	El DKIM no está habilitado por identidad.	Easy DKIM en SES
Punto fuerte del DKIM	La longitud de la clave de firma DKIM es inferior a 2048 bits.	La longitud de la clave de firma DKIM no utiliza al menos 2048 bits.	Easy DKIM en SES
Validación de registros DNS de DKIM	La verificación de DKIM ha fallado.	Tras buscar e intentar validar la clave, se determinó que los registros CNAME del DKIM no eran válidos.	Verificar la identidad de un dominio DKIM con tu proveedor de DNS
Configuración de DMARC	No se encontró la configuración de DMARC.	Faltan los registros TXT de DMARC.	Configuración de la política de DMARC en su dominio
Comprobación del formato de registro DNS de DMARC	No se pudo analizar la configuración de DMARC.	Se encontró un formato no válido para los registros TXT de DMARC.	Configuración de la política de DMARC en su dominio
Configuración DKIM de DMARC	No se encontró el registro DKIM.	No se encontró ningún registro DKIM para cumplir con el DMARC.	Cumplir con el DMARC a través del DKIM

Tipo de verificación	Mensaje del asesor	¿Por qué te alerta el asesor	Más información
Configuración DKIM de DMARC	El registro DKIM no está alineado.	El dominio especificado en la firma DKIM no se alinea (no coincide) con el dominio de la dirección de origen.	Cumple con el DMARC a través del DKIM
Configuración SPF	No se encontró el registro SPF.	Falta el registro TXT SPF para el dominio MAIL FROM personalizado.	Configurando tu dominio MAIL FROM personalizado
Se ha configurado el SPF «include»	No se encontró el registro SPF para Amazon SES.	`include:amazonses.com` falta en el registro TXT del SPF.	Configurando tu dominio MAIL FROM personalizado
Se ha configurado la aplicación del SPF	Falta el calificador SPF all.	`~all`falta en el registro TXT del SPF.	Configurando tu dominio MAIL FROM personalizado
Validación de la aplicación del SPF	Se encontró un problema de configuración del SPF.	No se pudo detectar el registro SPF MX requerido en un plazo de 72 horas.	Estado de configuración de MAIL FROM personalizado
Configurado en BIMI	No se ha encontrado ni configurado el registro BIMI sin el selector predeterminado.	Faltan registros BIMI TXT o no tienen el atributo selector.	Configuración de BIMI

Tipo de verificación	Mensaje del asesor	¿Por qué te alerta el asesor	Más información
Validación del formato BIMI	El BIMI tiene un registro TXT mal formado.	Se determinó que el registro TXT BIMI estaba mal configura do tras comprobar la presencia y el formato válido de: la versión, la URL del certificado y la URL del logotipo.	Configuración de BIMI

Uso del asesor de Virtual Deliverability Manager en la consola de Amazon SES

En el siguiente procedimiento se muestra cómo utilizar el asesor de Virtual Delivery en la consola de Amazon SES para resolver problemas de capacidad de entrega identificados mediante la consola de Amazon SES.

Para usar el asesor de Virtual Deliverability Manager para resolver problemas de capacidad de entrega y reputación

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. En el panel de navegación izquierdo, elija Advisor (Asesor) en Virtual Deliverability Manager.

   > **Note**
   >
   > El Advisor (Asesor) no estará visible si no ha habilitado Virtual Deliverability Manager para la cuenta. Para obtener más información, consulte the section called “Introducción”.

3. La tabla Open recommendations (Recomendaciones abiertas) se muestra de forma predeterminada. Las recomendaciones se clasifican por Impact (Impacto) (High/Low [Alto/bajo]), Identity name (Nombre de la identidad) (dominio de envío), Age (Antigüedad) (de la alerta) y Recommendation/Description (Recomendación/descripción) (problema identificado). En la barra

de búsqueda, filtre según el nivel de Impact (Impacto), la Category (Categoría) del problema de infraestructura o el Identity name (Nombre de la identidad) del dominio de envío.

4. Para solucionar un problema descrito en la columna Recommendation/Description (Recomendación/descripción), elija el enlace de la columna Resolve issue (Resolver problema) de esa fila e implemente la solución sugerida.

> **Note**
>
> Tras implementar una solución, el problema resuelto puede tardar hasta seis horas en reflejarse. Puede ver el problema resuelto en la pestaña Resolved recommendations (Recomendaciones resueltas).

Acceso a las recomendaciones de Virtual Deliverability Manager mediante la AWS CLI

En los siguientes ejemplos se muestra cómo acceder a las recomendaciones de Virtual Deliverability Manager con la AWS CLI.

Para acceder a las recomendaciones de Virtual Deliverability Manager mediante el AWS CLI

Puede utilizar la operación `ListRecommendations` en la API v2 de Amazon SES para mostrar las recomendaciones de capacidad de entrega. Puede llamar a esta operación desde la AWS CLI, como se muestra en los siguientes ejemplos.

- Muestre las recomendaciones para ver los problemas de capacidad de entrega:

```
aws --region us-east-1 sesv2 list-recommendations
```

- Aplique filtros para recuperar recomendaciones para un dominio específico de su propiedad:

```
aws --region us-east-1 sesv2 list-recommendations --cli-input-json file://list-recommendations.json
```

- El archivo de entrada tiene este aspecto:

```
{
  "PageSize":100,
  "Filter":{
```

```
    "RESOURCE_ARN": "arn:aws:ses:us-east-1:123456789012:identity/example.com"
   }
}
```

Configuración de Virtual Deliverability Manager

Puede consultar o cambiar la configuración de Virtual Deliverability Manager en la cuenta en cualquier momento. Puede habilitar o desactivar Virtual Deliverability Manager y especificar un modo de activación o desactivación para el seguimiento de las interacciones y la entrega compartida optimizada a nivel de cuenta de Virtual Deliverability Manager a través de la consola de Amazon SES o la AWS CLI

Las opciones de Virtual Deliverability Manager también se proporcionan en el nivel del conjunto de configuración para que pueda definir configuraciones personalizadas sobre cómo un conjunto de configuración utilizará el seguimiento de las interacciones y la entrega compartida optimizada invalidando la forma en que se han definido en Virtual Deliverability Manager. Esto le concede la flexibilidad de personalizar el envío de correos electrónicos para campañas de correo electrónico específicas. Por ejemplo, puede habilitar el seguimiento de las interacciones y la entrega compartida optimizada para el correo electrónico de marketing y desactivarlos para el correo electrónico transaccional.

Cambio de la configuración de la cuenta de Virtual Deliverability Manager con la consola de Amazon SES

El siguiente procedimiento muestra cómo cambiar la configuración de la cuenta de Virtual Deliverability Manager con la consola de Amazon SES.

Para cambiar la configuración de la cuenta de Virtual Deliverability Manager con la consola de Amazon SES

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación izquierdo, elija Settings (Configuración) en Virtual Deliverability Manager.

   Se abre la página de Virtual Deliverability Manager settings (Configuración de Virtual Deliverability Manager). El panel de Subscription overview (Información general de la suscripción) indica el estado de Virtual Deliverability Manager y el panel de Additional settings

(Configuración adicional) indica el estado del Engagement tracking (Seguimiento de las interacciones) y la Optimized shared delivery (Entrega compartida optimizada).

3. Para cambiar la configuración de Engagement tracking (Seguimiento de las interacciones) o de Optimized shared delivery (Entrega compartida optimizada):

   a. En el panel de Additional settings (Configuración adicional), elija Edit (Editar).

   b. Seleccione el botón de radio correspondiente para activar o desactivar cualquiera de las características y, a continuación, elija Submit settings (Enviar configuración).

      La página de Virtual Deliverability Manager settings (configuración de Virtual Deliverability Manager) muestra un resumen de los cambios en el panel de Additional settings (Configuración adicional).

      > **Note**
      >
      > Las opciones de Engagement tracking (Seguimiento de las interacciones) que defina aquí o en las anulaciones del conjunto de configuración de Virtual Deliverability Manager, controlan si informar o no sobre las aperturas y los clics en el panel de control de Virtual Deliverability Manager; no afectan a las configuraciones de destino de eventos que publican los eventos de apertura y clic. Por ejemplo, si tiene desactivado el seguimiento de las interacciones aquí, no desactivará la publicación de eventos de apertura y clic que haya configurado aquí en SES event destinations (Destinos de eventos de SES).

4. (Opcional) Para definir la configuración personalizada sobre cómo un conjunto de configuración usa el seguimiento de la interacciones y la entrega compartida optimizada invalidando la forma en que se han definido en Virtual Deliverability Manager, haga referencia a las opciones de Virtual Deliverability Manager mientras se crea o edita un conjunto de configuraciones.

5. Para desactivar Virtual Deliverability Manager:

   a. En el panel de Subscription overview (Información general de la suscripción), elija Disable Virtual Deliverability Manager (Desactivar Virtual Deliverability Manager).

   b. En la ventana emergente Disable Virtual Deliverability Manager? (¿Desactivar Virtual Deliverability Manager?), escriba `Disable` en el campo de confirmación y, a continuación, elija Disable Virtual Deliverability Manager (Desactivar Virtual Deliverability Manager).

   c. Se muestra un banner que confirma que ha desactivado Virtual Deliverability Manager.

6. Para volver a habilitar Virtual Deliverability Manager, consulte the section called “Introducción”.

Cambio de la configuración de la cuenta de Virtual Deliverability Manager con la AWS CLI

Puede cambiar la configuración de la cuenta de Virtual Deliverability Manager con la AWS CLI.

Para cambiar la configuración de la cuenta de Virtual Deliverability Manager con la AWS CLI

Puede utilizar las operaciones `PutAccountVdmAttributes` y `PutConfigurationSetVdmOptions` en la API v2 de Amazon SES para cambiar la configuración de Virtual Deliverability Manager. Puede llamar a esta operación desde la AWS CLI, como se muestra en los siguientes ejemplos.

- Habilite o desactive el seguimiento de las interacciones, la entrega compartida optimizada o ambos mediante un archivo de entrada:

  ```
  aws --region us-east-1 sesv2 put-account-vdm-attributes --cli-input-json file://
  attributes.json
  ```

  En este ejemplo, donde el seguimiento de las interacciones está `ENABLED` y la entrega compartida optimizada está `DISABLED`, el archivo de entrada tiene un aspecto similar al siguiente:

  ```
  {
      "VdmAttributes": {
          "VdmEnabled": "ENABLED",
          "DashboardAttributes": {
              "EngagementMetrics": "ENABLED"
          },
          "GuardianAttributes": {
              "OptimizedSharedDelivery": "DISABLED"
          }
      }
  }
  ```

  Puede encontrar más información sobre los valores de los parámetros y los tipos de datos relacionados enlazando el tipo de datos `VdmAttributes` de la referencia de la API v2 de Amazon SES.

- Defina configuraciones personalizadas sobre la forma en que un conjunto de configuración utilizará el seguimiento de las interacciones y la entrega compartida optimizada invalidando la forma en que se han definido en Virtual Deliverability Manager:

```
aws --region us-east-1 sesv2 put-configuration-set-vdm-options --cli-input-json
 file://config-set.json
```

En este ejemplo, en el que un conjunto de configuración llamado ejemplo tiene habilitados el seguimiento de las participaciones y la entrega compartida optimizada, el archivo de entrada tiene un aspecto similar al siguiente:

```
{
    "ConfigurationSetName": "example",
    "VdmOptions": {
        "DashboardOptions": {
            "EngagementMetrics": "ENABLED"
        },
        "GuardianOptions": {
            "OptimizedSharedDelivery": "ENABLED"
        }
    }
}
```

Para obtener más información sobre valores de parámetros y tipos de datos relacionados, consulte el tipo de datos `VdmOptions` en la referencia de la API v2 de Amazon SES.

- Para verificar el resultado:

```
aws –region us-east-1 sesv2 get-configuration-set –configuration-set-name example
```

- No especificar las opciones `DashboardOptions` o `GuardianOptions` en el nivel del conjunto de configuración da como resultado la configuración en el nivel de cuenta de Virtual Deliverability Manager que se aplica al tráfico enviado a través de ese conjunto de configuración.

Administrador de correo para Amazon SES

Mail Manager es un conjunto de funciones de pasarela de correo electrónico de Amazon SES diseñadas para ayudarlo a fortalecer la infraestructura de correo electrónico de su organización, simplificar la administración del flujo de trabajo del correo electrónico y agilizar el control del cumplimiento del correo electrónico. Se integra con su infraestructura existente, puede conectar diferentes aplicaciones empresariales y automatiza el procesamiento del correo entrante. Mail Manager también actúa como primera línea de defensa para mantener un sistema de correo electrónico en buen estado, ya que administra de manera eficiente el tráfico de correo electrónico y mejora el cumplimiento de su capacidad de archivado de correo electrónico.

Junto con las capacidades actuales de Amazon SES, Mail Manager incluye las siguientes funciones que admiten el tráfico entrante:

- Punto final de entrada: un componente clave de la infraestructura que utiliza políticas y reglas de filtrado que puede configurar para determinar qué correos electrónicos deben permitirse la entrada a su organización y cuáles deben rechazarse.
- Políticas y conjuntos de reglas de tráfico: permita a los administradores de correo electrónico definir y aplicar reglas para administrar el tráfico de correo entrante con políticas y reglas altamente personalizables que pueden ordenar, categorizar, priorizar y realizar acciones en los correos electrónicos en función de un amplio conjunto de condiciones y excepciones que usted defina. Este filtrado inteligente, combinado con flujos de trabajo automatizados, ayuda a agilizar la administración del correo electrónico, mejorar la eficiencia y garantizar el cumplimiento de las políticas de correo electrónico de la organización.
- Retransmisión SMTP: redirige el tráfico de correo electrónico a otros servidores SMTP en función de los criterios que defina en las reglas mediante la conexión de los sistemas de correo electrónico internos, y agiliza la administración del correo electrónico con el reenvío automático. La posibilidad de distribuir el tráfico entre varios servidores y puertas de enlace permite a su organización gestionar el tráfico de correo electrónico de gran volumen de forma eficaz, incluso en entornos híbridos.
- Archivado del correo electrónico: guarda y protege sus correos electrónicos al almacenar los datos en un almacenamiento persistente y seguro a largo plazo, y le permite buscar y archivar rápidamente el correo electrónico. Proporciona archivado a tiempo completo a nivel empresarial sin aumentar los requisitos de almacenamiento de su servidor de buzones de correo.
- Complementos de correo electrónico: conjunto de herramientas de seguridad especializadas de proveedores aprobados por SES que se pueden utilizar para gestionar el correo electrónico que

llega a su terminal de entrada, así como para ofrecer opciones de enrutamiento en función de los resultados de seguridad. Estas herramientas son soluciones certificadas de seguridad, inteligencia y cumplimiento que están listas para integrarse en su flujo de trabajo de correo electrónico y se pueden activar directamente desde la consola de Mail Manager.

Cómo empezar a usar Mail Manager

Para empezar a utilizar Mail Manager, un asistente de incorporación en la consola de Amazon SES le explicará los pasos necesarios para activar Mail Manager en su cuenta. Consulte the section called “Introducción”.

Temas

- Cómo empezar a usar Mail Manager
- Puntos finales de entrada
- Políticas de tráfico y declaraciones de políticas
- Conjuntos de reglas y reglas
- Relé SMTP
- Archivado de correo electrónico
- Complementos de correo electrónico
- Políticas de permisos para Mail Manager

Cómo empezar a usar Mail Manager

Para empezar a utilizar Amazon SES Mail Manager, puede utilizar el asistente Get Started with Mail Manager de la consola de Amazon SES, donde creará un punto de entrada y lo configurará con una política de tráfico y un conjunto de reglas.

Un punto final de entrada es el primer elemento fundamental para configurar Mail Manager. Se trata de un componente clave de la infraestructura que utiliza:

- Políticas de tráfico: una política de tráfico contiene declaraciones de políticas que usted define para ordenar el correo entrante permitiendo o bloqueando tipos específicos de correo electrónico cuando se cumplen las condiciones de la declaración de política.
- Conjuntos de reglas: un conjunto de reglas contiene reglas que usted define para realizar acciones en el correo electrónico que permite entrar cuando se cumplen las condiciones de la regla.

Sin embargo, parte de la creación de un punto final de entrada consiste en seleccionar una política de tráfico y un conjunto de reglas que ya se hayan creado y, a continuación, asignarlos al punto final de entrada. Los pasos del siguiente procedimiento le indicarán el orden correcto de configuración del primer punto final de entrada.

Cómo empezar a usar Mail Manager mediante la consola de SES

El siguiente procedimiento le muestra cómo empezar a utilizar Mail Manager mediante la consola SES.

Para empezar a utilizar Mail Manager mediante la consola Amazon SES

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. En el panel de navegación izquierdo, selecciona Mail Manager y selecciona cualquiera de los botones Comenzar con Mail Manager de la página de información general de Mail Manager.
3. En la página de configuración, selecciona Crear política de tráfico en la tarjeta Crear una política de tráfico.

    a. Complete el flujo de trabajo en la página Crear una política de tráfico. Si necesita información adicional, consultethe section called “Creación de políticas y declaraciones de políticas de tráfico (consola)”.

    b. Tras crear su primera política de tráfico y sus primeras declaraciones de políticas, utilice el botón de retroceso del navegador para volver a la página de configuración o seleccione Configurar en Mail Manager, en el panel de navegación izquierdo.
4. En la página Configurar, selecciona Crear conjunto de reglas en la tarjeta Crear un conjunto de reglas.

    a. Complete el flujo de trabajo en la página Crear un conjunto de reglas. Si necesita información adicional, consultethe section called “Creación de conjuntos de reglas y reglas (consola)”.

    b. Tras crear el primer conjunto de reglas y reglas, utilice el botón de retroceso del navegador para volver a la página de configuración o seleccione Configurar en Mail Manager, en el panel de navegación izquierdo.
5. Ahora que has creado tu primer conjunto de políticas y reglas de tráfico, podrás crear tu primer punto de acceso. En la página Configurar, selecciona Crear punto final de entrada en la tarjeta Crear un punto final de entrada.

- Parte del flujo de trabajo de la página de punto final de entrada de correo electrónico consistirá en asignar el conjunto de políticas y reglas de tráfico que acabas de crear al punto final de entrada. Si necesita información adicional, consulte. the section called “Crear un punto final de entrada (consola)”

Una vez creado el primer terminal de entrada, puede empezar a usar Mail Manager y utilizar sus demás funciones, como los relés SMTP y el archivado de correo electrónico. También puedes crear puntos de enlace de entrada adicionales con políticas de tráfico y conjuntos de reglas únicos para personalizar aún más la forma en que administras todo el correo entrante.

Puntos finales de entrada

Un punto final de entrada es el componente clave de la infraestructura de Mail Manager que recibe, enruta y administra el correo electrónico mediante políticas y reglas que usted configura para determinar qué correos electrónicos deben rechazarse, cuáles deben permitirse y cuáles deben tomarse medidas al respecto.

Cada punto de enlace de entrada tiene su propia política de tráfico para determinar qué correos electrónicos bloquear o permitir, y su propio conjunto de reglas para realizar acciones en el correo electrónico que permite la entrada; por lo tanto, al crear varios puntos de enlace de entrada, puede delegar en cada uno de ellos la administración y enrutamiento de tipos específicos de correo electrónico. Este nivel de granularidad le ayudará a crear un sistema de administración del correo electrónico que se adapte a las necesidades de su empresa.

Flujo de trabajo imprescindible para crear un punto final de entrada

Al crear su punto final de entrada, debe asignarle una política de tráfico y un conjunto de reglas que ya se hayan creado. Por lo tanto, el flujo de trabajo para crear un punto final de entrada debe estar en el siguiente orden:

1. Comience por crear una política de tráfico para determinar el correo electrónico que desea bloquear o permitir. Para obtener más detalles, consulte the section called “Creación de políticas y declaraciones de políticas de tráfico (consola)”.
2. A continuación, crea un conjunto de reglas para realizar acciones en el correo electrónico al que permitas entrar. Para obtener más detalles, consulte the section called “Creación de conjuntos de reglas y reglas (consola)”.

3. Por último, cree su punto final de entrada y asígnele la política de tráfico y el conjunto de reglas que acaba de crear o cualquier otro que haya creado anteriormente.

Una vez creado el punto final de entrada, debe configurarlo con el entorno que está utilizando para recibir correo electrónico, ya sea la configuración de un cliente SMTP local o de un host de dominio DNS basado en la web. Esto se analiza más adelante en. the section called “Configuración de su entorno de ”

Configuración del entorno para utilizar un punto final de entrada

Uso del registro «A»

Al crear un punto final de entrada, se generará un registro «A» para el punto final y su valor se mostrará en la pantalla de resumen del punto final de entrada en la consola de SES. La forma en que utilice el valor de este registro depende del tipo de punto final que haya creado y de su caso de uso:

- Punto de acceso abierto: el correo enviado a tu dominio se enviará directamente a tu punto de acceso, sin necesidad de autenticación.
  - Copia y pega el valor del registro «A» directamente en la configuración SMTP de un cliente SMTP local o en un registro MX de tu dominio en tu configuración de DNS.
- Punto final autenticado: el correo enviado a tu dominio debe provenir de remitentes autorizados con los que hayas compartido tus credenciales SMTP, como los servidores de correo electrónico locales.
  - Copia y pega el valor del registro «A» directamente en la configuración SMTP de un cliente SMTP local, así como tu nombre de usuario y contraseña.

Si utilizas un registro MX en tu configuración, ten en cuenta que, si bien cada proveedor de DNS tiene procedimientos e interfaces diferentes para configurar los registros, la información clave que necesitas incluir en la configuración de DNS se muestra en el siguiente ejemplo:

Todos los correos electrónicos que envíes a recipient@marketing.example.com irán a tu punto de acceso porque has introducido el registro «A» del punto de acceso como valor de un registro MX en la configuración de DNS de tu dominio:

- Dominio: `marketing.example.com`
- Valor de registro MX: `890123abcdef.ghijk.mail-manager-smtp.amazonaws.com` (este es el valor de registro «A» copiado del punto final de entrada).

- Prioridad: `10`

El procedimiento de la siguiente sección le explicará cómo crear un punto final de entrada en la consola de SES.

Crear un punto final de entrada en la consola de SES

El siguiente procedimiento le muestra cómo utilizar la página de puntos de enlace de entrada de la consola de SES para crear puntos de enlace de entrada y administrar los que ya ha creado.

Para crear y gestionar los puntos finales de entrada mediante la consola

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. En el panel de navegación izquierdo, selecciona los puntos de enlace de Ingress en Mail Manager.
3. En la página de puntos finales de entrada, selecciona Crear punto final de entrada.
4. En la página Crear un nuevo punto final de entrada, introduce un nombre único para tu punto final de entrada.
5. Elija si será un punto final abierto o autenticado.

    - Si eliges Autenticado, selecciona Contraseña SMTP e introduce una contraseña, o Secreto y selecciona uno de tus secretos del ARN secreto. Si selecciona un secreto creado anteriormente, debe contener las políticas indicadas en los pasos siguientes para crear un secreto nuevo.
    - Tienes la opción de crear un secreto nuevo. Para ello, selecciona Crear nuevo. Se abrirá la AWS Secrets Manager consola en la que podrás seguir creando una clave nueva:

    a. Selecciona Otro tipo de secreto en Tipo de secreto.

    b. En el par clave/valor, introduzca `password` la clave y su contraseña real para el valor.

    > **Note**
    >
    > En el caso de la clave, solo debe introducirla `password` (cualquier otra cosa provocará un error en la autenticación).

c. Seleccione Añadir nueva clave para crear una clave gestionada por el cliente (CMK) de KMS en la clave de cifrado; se abrirá la AWS KMS consola.

d. Seleccione Crear clave en la página de claves administradas por el cliente.

e. Mantenga los valores predeterminados en la página de configuración de claves y seleccione Siguiente.

f. Introduzca un nombre para la clave en Alias (si lo desea, puede añadir una descripción y una etiqueta), seguido de Siguiente.

g. Seleccione los usuarios (que no sean usted) o los roles a los que desee permitir que administren la clave en Administradores clave y, a continuación, en Siguiente.

h. Seleccione los usuarios (que no sean usted) o los roles a los que desee permitir que usen la clave en Usuarios clave y, a continuación, en Siguiente.

i. Cópielo y péguelo Política CMK de KMS en el editor de texto JSON de políticas clave del `"statement"` nivel agregándolo como una declaración adicional separada por una coma. Sustituya la región y el número de cuenta por los suyos.

j. Seleccione Finalizar.

k. Selecciona la pestaña del navegador en la que tengas abierta la página AWS Secrets Manager Guardar una nueva página secreta y selecciona el icono de actualización (flecha circular) situado junto al campo de la clave de cifrado. A continuación, haz clic dentro del campo y selecciona la clave recién creada.

l. Introduce un nombre en el campo Nombre secreto de la página Configurar secretos.

m. Seleccione Editar permisos en Permisos de recursos.

n. Cópielo y péguelo Política de recursos de Secrets en el editor de texto JSON de permisos de recursos y sustituya la región y el número de cuenta por los suyos. (Asegúrese de eliminar cualquier código de ejemplo del editor).

o. Selecciona Guardar seguido de Siguiente.

p. Si lo desea, configure la rotación seguida de Siguiente.

q. Revisa y guarda tu nuevo secreto seleccionando Guardar.

r. Seleccione la pestaña de su navegador en la que tenga abierta la página SES Crear un nuevo punto final de entrada y, a continuación, elija Actualizar lista y, a continuación, seleccione su secreto recién creado en Secret ARN.

6. Seleccione una política de tráfico para determinar el correo electrónico que desea bloquear o permitir.

7. Seleccione un conjunto de reglas que contenga las acciones de reglas que desee realizar en el correo electrónico al que permite la entrada.
8. Seleccione Crear punto final de entrada.
9. En general, aparecerá «Aprovisionamiento» mientras se crea el punto de acceso. Actualice la página hasta que aparezca «Activo» y el campo ARecord contenga un valor. Copie el valor del registro «A» y péguelo en la configuración de DNS o en el cliente SMTP, tal y como se indica en la sección. Configuración de su entorno de
10. Puede ver y administrar los puntos de enlace de entrada que ya ha creado desde la página de puntos de enlace de entrada. Si hay un punto final de entrada que quieras eliminar, selecciona su botón de radio y, a continuación, selecciona Eliminar.
11. Para editar un punto final de entrada, selecciona su nombre para abrir su página de resumen:

    - Para cambiar el estado activo del punto final, seleccione Editar en detalles generales y, a continuación, Guardar cambios.
    - Para seleccionar un conjunto de reglas o una política de tráfico diferente, seleccione Editar en el conjunto de reglas o en la política de tráfico y, a continuación, seleccione Guardar cambios.

Políticas de tráfico y declaraciones de políticas

Una política de tráfico es un contenedor de declaraciones de políticas que se asigna a un punto de entrada para que pueda clasificar el correo entrante al permitir o bloquear tipos específicos de correo electrónico cuando se cumplen las condiciones de las declaraciones de política. Varios puntos finales de entrada pueden utilizar una política de tráfico.

> **Tip**
>
> Puede pensar en una política de tráfico como un «conjunto de filtros» y en una declaración de política como un «filtro». La política de tráfico (conjunto de filtros) contiene las políticas (filtros) que se utilizan para filtrar el correo entrante.

Al crear una política de tráfico, tiene la opción de establecer un tamaño máximo de mensaje (en bytes). Cuando un mensaje supera ese tamaño, se descarta inmediatamente. Cuando se configura, actúa como un filtro de «primer paso». A continuación, establece la acción predeterminada para permitir o bloquear el correo electrónico que no cumpla con las condiciones de sus declaraciones de política; considérelo como una acción de «catch all» para la política de tráfico.

Las declaraciones de política también se crean con una acción de permiso o bloqueo que se lleva a cabo cuando se cumplen las condiciones de las declaraciones. Para crear las condiciones, seleccione un protocolo de correo electrónico y un operador condicional para el valor que introduzca y que debe coincidir con el mensaje entrante para que la declaración de política lo permita o bloquee. Cada declaración de política puede tener varias condiciones.

Una política de tráfico puede contener varias declaraciones de política y ejecutarlas en un orden que se basa en la jerarquía implícita de la forma en que evalúa el correo electrónico:

- Tamaño máximo del mensaje: si se establece este parámetro opcional, cualquier mensaje que supere este tamaño se descarta inmediatamente, sin tener en cuenta las declaraciones de política.
- Declaraciones de política que bloquean: estas declaraciones se evalúan primero y bloquean cualquier mensaje que cumpla las condiciones de la declaración.
- Declaraciones de política que lo permiten: estas declaraciones se evalúan a continuación y admiten cualquier mensaje que cumpla las condiciones de la declaración.
- Acción predeterminada de la política de tráfico: el resto de los mensajes que no están incluidos en las declaraciones de la política se permiten o bloquean en función de cómo se haya definido este parámetro.

Una política de tráfico es un recurso independiente que puede ser utilizado por más de un punto final de entrada, pero las declaraciones de política pertenecen exclusivamente a la política de tráfico en la que se crearon. Por lo tanto, primero debe crear una política de tráfico, o editar una existente, antes de poder crear declaraciones de política para evaluar el correo electrónico que llega a su punto final de entrada.

El procedimiento de la siguiente sección explica cómo crear políticas de tráfico y sus declaraciones de políticas en la consola de SES.

Creación de políticas de tráfico y declaraciones de políticas en la consola de SES

El siguiente procedimiento le muestra cómo usar la página de políticas de tráfico de la consola de SES para crear políticas de tráfico y sus declaraciones de políticas, y administrar las que ya ha creado.

Para crear y administrar políticas y declaraciones de políticas de tráfico mediante la consola

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. En el panel de navegación izquierdo, selecciona Políticas de tráfico en Mail Manager.
3. En la página Políticas de tráfico, selecciona Crear política de tráfico.
4. En la página Crear una política de tráfico, introduce un nombre único para tu política de tráfico.
5. (Opcional) Si desea descartar los mensajes que superen un tamaño determinado, introduzca un valor en bytes en el campo Tamaño máximo de mensaje.
6. Como opción predeterminada, elija si la política de tráfico es permitir o denegar (bloquear) los mensajes que no cumplan (no estén contemplados) en las condiciones de sus declaraciones de política.
7. Seleccione Añadir nueva declaración de política para crear una declaración para su política de tráfico.
8. Elija Permitir o Denegar (bloquear) para la acción que se realizará cuando se cumplan las condiciones de la declaración.
9. Cree una condición seleccionando un protocolo de correo electrónico y un operador condicional para el valor que introduzca. Seleccione Añadir nueva condición si desea añadir más condiciones a esta declaración de política. Para obtener más información sobre una propiedad condicionada y sus operadores y valores válidos, consulta la referencia de condiciones de la declaración de política.

   - Si estás suscrito a un complemento de correo electrónico, podrás seleccionarlo aquí como protocolo de correo electrónico.
10. Si quieres añadir más declaraciones y condiciones de política, repite los pasos 7 a 9 anteriores.
11. Cuando haya terminado de crear las declaraciones de política y sus condiciones, seleccione Crear política de tráfico.
12. Puedes ver y administrar las políticas de tráfico que ya has creado en la página de políticas de tráfico. Si hay una política de tráfico que quieras eliminar, selecciona su botón de radio y, a continuación, Eliminar.
13. Para editar las propiedades de una política de tráfico o cualquiera de sus declaraciones de política, selecciona su nombre para abrir su página de descripción general y, desde aquí, selecciona Editar.
14. En los detalles de la política de tráfico, puedes cambiar el tamaño máximo de los mensajes y la acción predeterminada.

15. En cualquiera de los contenedores de declaraciones de política, puedes cambiar la propiedad de permitir/denegar y editar cualquiera de las condiciones. También puede eliminar las declaraciones y condiciones de política, así como añadir otras nuevas.
16. Cuando hayas terminado de editar todos los cambios, selecciona Guardar cambios para guardar los cambios.

Referencia para las condiciones de la declaración de política

Condiciones de la declaración de política

La siguiente tabla de referencia enumera todos los protocolos de declaración de política que están disponibles para crear una condición de declaración de política. Al seleccionar el tipo de expresión de un protocolo, accederá a su página de referencia en la referencia de la API de SES Mail Manager, en la que se enumeran todos los operadores disponibles y los valores válidos para ese protocolo.

Condiciones de la declaración de política: protocolos, operadores y valores

Protocolo	Tipo de expresión
Dirección del destinatario	Operadores y valores válidos para expresiones de cadenas
Rango de direcciones IP del remitente	Operadores y valores válidos para las expresiones IP
Versión del protocolo TLS	Operadores y valores válidos para las expresiones del protocolo TLS
Abusix Mail Intelligence (si está suscrito) Lista de dominios bloqueados de Spamhaus (si está suscrito)	Operadores y valores válidos para expresiones booleanas

Conjuntos de reglas y reglas

Los conjuntos de reglas son contenedores de reglas que se asignan a un punto final de entrada para que este pueda realizar acciones con el correo electrónico admitido por la política de tráfico del punto final de entrada. Varios puntos finales de entrada pueden usar un conjunto de reglas.

Las reglas indican al punto final de entrada cómo gestionar el correo entrante mediante la ejecución de las acciones definidas en la regla cuando los mensajes cumplen las condiciones de la regla. Cada regla puede tener varias condiciones y acciones. Las reglas que cree dentro de un conjunto de reglas se ejecutan en el orden que especifique dentro del conjunto de reglas.

Para crear las condiciones de la regla, debe seleccionar una propiedad de correo electrónico y un operador condicional para el valor que introduzca y que debe coincidir con el mensaje antes de que la regla ejecute sus acciones. Usted define las acciones que se van a llevar a cabo, así como su orden de ejecución.

Para una mayor granularidad, las reglas también pueden contener excepciones definidas de forma similar a las condiciones, pero en este caso, se define una condición que el mensaje no debe cumplir. Las condiciones y las excepciones funcionan de forma independiente; si lo desea, puede crear una regla que contenga únicamente excepciones, así como mezclar condiciones y excepciones.

Debido a la gran granularidad de cómo se pueden definir las reglas dentro de un conjunto de reglas, se proporciona la siguiente lista para ayudar a ilustrar la relación entre los componentes del conjunto de reglas:

- Los conjuntos de reglas contienen:
  - Reglas: puede definir el orden en el que se ejecutan las reglas dentro del conjunto de reglas.

    Las reglas contienen:

    - Condiciones: la regla se aplica si el mensaje coincide con la evaluación de las condiciones; y si la regla tiene excepciones, consulte a continuación.
    - Excepciones: la regla se aplica si el mensaje no coincide con la evaluación de las excepciones y si la regla tiene condiciones, consulte lo anterior.
    - Acciones: las acciones se activan cuando se aplica la regla: todas las condiciones coinciden y ninguna de las excepciones.

      Puede definir el orden en el que se ejecutan las acciones dentro de la regla.

Como cada regla puede tener varias condiciones, excepciones y acciones, y el hecho de que puede definir el orden en que se ejecutan las reglas y las acciones, esto le permite crear una solución de gestión del correo electrónico muy personalizada y automatizada que se adapte a sus requisitos empresariales específicos.

Un conjunto de reglas es un recurso independiente que puede ser utilizado por más de un punto final de entrada, pero las reglas pertenecen exclusivamente al conjunto de reglas en el que se crearon. Por lo tanto, primero debe crear un conjunto de reglas o editar uno existente antes de poder crear reglas que actúen cuando el correo electrónico llegue a su punto final de entrada.

El procedimiento de la siguiente sección te explicará cómo crear conjuntos de reglas y sus reglas en la consola de SES.

Creación de conjuntos de reglas y reglas en la consola de SES

El siguiente procedimiento le muestra cómo utilizar la página de conjuntos de reglas de la consola de SES para crear conjuntos de reglas y sus reglas, y administrar los que ya ha creado.

Para crear y gestionar conjuntos de reglas y reglas mediante la consola

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. En el panel de navegación izquierdo, selecciona Conjuntos de reglas en Mail Manager.
3. En la página Conjuntos de reglas, elija Crear conjunto de reglas e introduzca un nombre único para el conjunto de reglas.
4. En la página de descripción general del conjunto de reglas, selecciona Editar y, a continuación, selecciona Crear nueva regla en la página de edición.
5. En la barra lateral de detalles de la regla, introduce un nombre único para la regla.
6. Selecciona Añadir nueva condición para crear una condición con la que el mensaje deba coincidir o marca la casilla EXCEPTO en el caso de: seguida de Añadir nueva excepción para crear una condición con la que el mensaje no debe coincidir.
7. Cree la condición o excepción seleccionando una propiedad de correo electrónico y un operador condicional para el valor que introduzca. Seleccione Añadir nueva condición o Añadir nueva excepción si desea añadir más condiciones o excepciones a esta regla. Para obtener más información sobre una propiedad de condición y sus operadores y valores válidos, consulte la referencia de condiciones de la regla.

   - Si estás suscrito a un complemento de correo electrónico, podrás seleccionarlo aquí como propiedad de correo electrónico.
8. Selecciona Añadir nueva acción para definir la acción que se debe realizar cuando se cumplan las condiciones de la regla o las excepciones no coincidan. Para añadir más acciones a realizar,

selecciona Añadir nueva acción. Para obtener más información sobre las acciones y sus parámetros, consulta la referencia sobre las acciones de las reglas.

- Para ejecutar las acciones de la regla Escribir en S3, Entregar en el buzón y Enviar a Internet, necesitará tener Políticas de acción de reglas habilitadas las acciones de la regla en su cuenta; de lo contrario, la acción de la regla fallará.
- Al crear dos o más acciones, se muestran las flechas arriba/abajo para que puedas establecer el orden de ejecución.

9. Cuando haya terminado de crear las condiciones, excepciones y acciones de la regla, para guardarla en su conjunto de reglas, seleccione Guardar conjunto de reglas, ubicado en el panel Editar conjunto de reglas de la izquierda.
10. Si desea añadir más reglas al conjunto de reglas, repita los pasos 4 a 9 anteriores.

    - Al crear dos o más reglas, se muestran las flechas arriba/abajo en la columna Reordenar del conjunto de reglas para que pueda establecer el orden de ejecución.

11. Puede ver y administrar los conjuntos de reglas que ya ha creado desde la página de conjuntos de reglas. Si hay un conjunto de reglas que quieras eliminar, selecciona su botón de opción y, a continuación, selecciona Eliminar.
12. Para editar un conjunto de reglas, selecciona su nombre para abrir su página de información general. Desde aquí, selecciona Editar, donde podrás reordenar la ejecución de sus reglas, añadir más reglas seleccionando Crear nueva regla o eliminar una regla seleccionando su botón de radio seguido de Eliminar.
13. Para editar una regla, selecciona su botón de radio. En cualquiera de los contenedores de la barra lateral de detalles de la regla, puede editar cualquiera de las condiciones o excepciones y cambiar o reordenar cualquiera de las acciones. También puedes eliminar condiciones, excepciones y acciones, así como añadir otras nuevas.
14. Cuando termines de editar todos los cambios, selecciona Guardar conjunto de reglas en el panel Editar conjunto de reglas de la izquierda para guardar los cambios.

Referencia para las condiciones y acciones de las reglas

Condiciones de la regla

La siguiente tabla de referencia muestra todas las propiedades de la regla que están disponibles para crear una condición (o excepción) de la regla y se clasifican por su tipo de expresión. Las propiedades de la regla que comparten el mismo tipo de expresión también comparten los mismos

operadores y valores. Al seleccionar el tipo de expresión de una propiedad, accederá a su página de referencia en la referencia de la API de SES Mail Manager, en la que se enumeran todos los operadores disponibles y los valores válidos para esa propiedad.

Condiciones de la regla: propiedades, operadores y valores

Propiedad	Tipo de expresión
Dirección de origen A la dirección Dirección CC Correo de Dirección del destinatario Asunto Hola	Operadores y valores válidos para expresiones de cadenas
Rango de IP	Operadores y valores válidos para las expresiones IP
Tamaño máximo del mensaje	Operadores y valores válidos para expresiones numéricas
DKIM SPF Trend Micro Virus Scanning (si está suscrito)	Operadores y valores válidos para las expresiones de veredicto
TLS Envuelto en TLS Lea el recibo	Operadores y valores válidos para expresiones booleanas
Política DMARC	Operadores y valores válidos para las expresiones DMARC

Acciones de reglas

En la siguiente tabla de referencia se enumeran todas las acciones de regla que se pueden realizar cuando se cumplen las condiciones de una regla o no se cumplen sus excepciones. Al seleccionar una acción, accederás a la página de referencia de la acción en la Referencia de la API de SES Mail Manager, en la que se enumeran los parámetros y sus formatos para la acción. En la tabla se utilizan los nombres de las acciones adoptados en la consola de Mail Manager; los nombres de las API pueden variar ligeramente.

> **Note**
>
> En algunas de las referencias a la API, habrá un `ActionFailurePolicy` parámetro que se puede configurar en Continuar o Descartar si la acción falla. Esto solo se aplica cuando se usa la API; cuando se usa la consola, `ActionFailurePolicy` se establece en el valor predeterminado de Continuar.

Acciones de la regla: acciones y parámetros

Acciones y sus parámetros	Descripción
Escribe a S3	Escribe el contenido MIME del correo electrónico en un bucket de S3.
Acción de retransmisión SMTP	Transmite el correo electrónico mediante SMTP a otro servidor SMTP específico.
Acción de archivar	Archiva el correo electrónico enviándolo a un archivo de Amazon SES.
Añadir encabezado	Añade un encabezado personalizado al correo electrónico recibido.
Los destinatarios del correo electrónico lo reescriben	Sustituye los destinatarios del sobre de correo electrónico por la lista de destinatarios indicada. Si la condición de esta acción se aplica solo a un subconjunto de destinatarios, solo se sustituirán esos destinatarios.

Acciones y sus parámetros	Descripción
Entregar al buzón	Envía el correo electrónico a un WorkMail buzón de Amazon.
Enviar a internet	Utiliza SES para enviar el correo electrónico a los destinatarios de la lista de destinatarios del correo electrónico.
Acción de soltar	En el caso de los correos electrónicos con varios destinatarios, si esta acción se aplica a uno o más de esos destinatarios (pero no a todos), se eliminarán de la lista de destinatarios del correo electrónico y se aplicará el procesamiento continuo de las normas a los demás destinatarios. Si esta acción se aplica a todos los destinatarios, el procesamiento de las reglas se detendrá, ya que todos los destinatarios se eliminarán de la lista de destinatarios y no recibirán el correo electrónico.

Relé SMTP

Como Mail Manager se implementa entre su entorno de correo electrónico (como Microsoft 365, Google Workspace o On-Premise Exchange) e Internet, Mail Manager utiliza retransmisores SMTP para enrutar los correos entrantes procesados por Mail Manager a su entorno de correo electrónico. También puede enrutar los correos salientes a otra infraestructura de correo electrónico, como otro servidor de Exchange o una pasarela de correo electrónico de terceros, antes de enviarlos a los destinatarios finales.

Un retransmisor SMTP es un componente vital de la infraestructura de correo electrónico, responsable de enrutar de manera eficiente los correos electrónicos entre servidores cuando se designa mediante una acción de regla definida en un conjunto de reglas.

En concreto, una retransmisión SMTP puede redirigir el correo entrante entre SES Mail Manager y una infraestructura de correo externa, como Exchange, pasarelas de correo electrónico locales o de terceros, entre otras. Los correos electrónicos entrantes a un punto de entrada se procesarán según

una regla que enrutará el correo electrónico especificado al retransmisor SMTP designado, el cual, a su vez, lo transmitirá a la infraestructura de correo electrónico externa definida en el retransmisor SMTP.

Cuando su terminal de entrada recibe correo electrónico, utiliza una política de tráfico para determinar qué correos electrónicos bloquear o permitir. El correo electrónico que permitas entrar pasa a un conjunto de reglas que aplica reglas condicionales para ejecutar las acciones que has definido para tipos específicos de correo electrónico. Una de las acciones de la regla que puedes definir es la acción de retransmisión SMTP: si seleccionas esta acción, el correo electrónico se transferirá al servidor SMTP externo definido en la retransmisión SMTP.

Por ejemplo, puede usar la acción SMTPRelay para enviar correo electrónico desde su punto de acceso a su servidor Microsoft Exchange local. Deberías configurar tu servidor de Exchange para que tuviera un punto final SMTP público al que solo se pueda acceder con determinadas credenciales. Al crear la retransmisión SMTP, introduce el nombre, el puerto y las credenciales del servidor de Exchange y asigna a la retransmisión SMTP un nombre único, por ejemplo, "». RelayToMyExchangeServer A continuación, crea una regla en el conjunto de reglas del terminal de entrada que diga: «Cuando la dirección de origen contenga 'gmail.com', ejecute la acción de retransmisión SMTP mediante la retransmisión SMTP llamada». RelayToMyExchangeServer

Ahora, cuando el correo de gmail.com llegue a tu terminal de entrada, la regla activará la acción de retransmisión SMTP y se pondrá en contacto con tu servidor de Exchange con las credenciales que proporcionaste al crear la retransmisión SMTP y entregará el correo electrónico a tu servidor de Exchange. Por lo tanto, el correo electrónico recibido de gmail.com se retransmite a tu servidor de Exchange.

Primero debes crear una retransmisión SMTP para poder designarla en una acción de regla. El procedimiento de la siguiente sección le explicará cómo crear un relé SMTP en la consola de SES.

Creación de un relé SMTP en la consola de SES

El siguiente procedimiento le muestra cómo utilizar la página de retransmisiones SMTP de la consola de SES para crear retransmisiones SMTP y administrar las que ya ha creado.

Para crear y administrar los relés SMTP mediante la consola

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. En el panel de navegación izquierdo, selecciona los relés SMTP en Mail Manager.

3. En la página de retransmisiones SMTP, selecciona Crear retransmisión SMTP.
4. En la página Crear retransmisión SMTP, introduce un nombre exclusivo para la retransmisión SMTP.
5. En función de si desea configurar una retransmisión SMTP entrante (no autenticada) o saliente (autenticada), siga las instrucciones correspondientes:

   Inbound

   Para configurar una retransmisión SMTP entrante

   1. Si la retransmisión SMTP se utiliza como puerta de enlace entrante para enrutar los correos electrónicos entrantes procesados por Mail Manager a su entorno de correo electrónico externo, primero tendrá que configurar el entorno de alojamiento del correo electrónico. Si bien cada proveedor de alojamiento de correo electrónico tiene su propia interfaz gráfica de usuario y su propio flujo de trabajo de configuración, los principios básicos para configurarlos para que funcionen con las puertas de enlace entrantes, como la retransmisión SMTP de Mail Manager, serán similares.

      Para ayudar a ilustrarlo, en las siguientes secciones se proporcionan ejemplos de cómo configurar Google Workspaces y Microsoft Office 365 para que funcionen con la retransmisión SMTP como puerta de enlace de entrada:

      - Configuración de Google Workspaces
      - Configuración de Microsoft Office 365

      Actualmente, SES solo admite retransmisiones SMTP entrantes (no autenticadas) para Google Workspaces y Microsoft Office 365.

      > **Note**
      >
      > Asegúrese de que los dominios de los destinos de sus destinatarios previstos sean identidades de dominio verificadas por SES. Por ejemplo, si desea enviar correos electrónicos a los destinatarios abc@example.com y support@acme.com, los dominios example.com y acme.com deben estar verificados en SES. Si el dominio de un destinatario no está verificado, SES no intentará entregar el correo electrónico al servidor SMTP público. Para

obtener más información, consulte the section called “Creación y verificación de identidades”.

2. Después de configurar Google Workspaces o Microsoft Office 365 para que funcionen con puertas de enlace entrantes, introduzca el nombre de host del servidor SMTP público con los valores siguientes correspondientes a su proveedor:

   - Espacios de trabajo de Google: `aspmx.l.google.com`
   - Microsoft Office 365: `<your_domain>.mail.protection.outlook.com`

     Sustituya los puntos por «-» en su nombre de dominio. Por ejemplo, si tu dominio es acme.com, debes escribir `acme-com.mail.protection.outlook.com`

3. Introduzca el número de puerto 25 para el servidor SMTP público.
4. Deje la sección Autenticación en blanco (no seleccione ni cree un ARN secreto).

Outbound

Para configurar una retransmisión SMTP saliente

1. Introduzca el nombre de host del servidor SMTP público al que desea que se conecte la retransmisión.
2. Introduzca el número de puerto del servidor SMTP público.
3. Configure la autenticación para su servidor SMTP seleccionando uno de sus secretos del ARN secreto. Si selecciona un secreto creado anteriormente, debe contener las políticas indicadas en los pasos siguientes para crear un secreto nuevo.

   - Tienes la opción de crear un secreto nuevo seleccionando Crear nuevo; se abrirá la AWS Secrets Manager consola donde podrás seguir creando una clave nueva:

     a. Selecciona Otro tipo de secreto en Tipo de secreto.

     b. Introduzca las siguientes claves y valores en pares clave/valor:

Clave	valor
`username`	mi_nombre de usuario

Clave	valor
`password`	mi_contraseña

> **Note**
>
> Para ambas claves, solo debe introducir `username` y `password` tal como se muestra (cualquier otra cosa provocará un error en la autenticación). Para los valores, introduzca su propio nombre de usuario y contraseña, respectivamente.

c. Seleccione Añadir nueva clave para crear una clave gestionada por el cliente (CMK) de KMS en la clave de cifrado; se abrirá la AWS KMS consola.

d. Seleccione Crear clave en la página de claves administradas por el cliente.

e. Mantenga los valores predeterminados en la página de configuración de claves y seleccione Siguiente.

f. Introduzca un nombre para la clave en Alias (si lo desea, puede añadir una descripción y una etiqueta), seguido de Siguiente.

g. Seleccione los usuarios (que no sean usted) o los roles a los que desee permitir que administren la clave en Administradores clave y, a continuación, en Siguiente.

h. Seleccione los usuarios (que no sean usted) o los roles a los que desee permitir que usen la clave en Usuarios clave y, a continuación, en Siguiente.

i. Copie y péguelo Política CMK de KMS en el editor de texto JSON de políticas clave del `"statement"` nivel agregándolo como una declaración adicional separada por una coma. Sustituya la región y el número de cuenta por los suyos.

j. Seleccione Finalizar.

k. Selecciona la pestaña del navegador en la que tengas abierta la página AWS Secrets Manager Guardar una nueva página secreta y selecciona el icono de actualización (flecha circular) situado junto al campo de la clave de cifrado. A continuación, haz clic dentro del campo y selecciona la clave recién creada.

l. Introduce un nombre en el campo Nombre secreto de la página Configurar secretos.

m. Seleccione Editar permisos en Permisos de recursos.

n. Cópielo y péguelo Política de recursos de Secrets en el editor de texto JSON de permisos de recursos y sustituya la región y el número de cuenta por los suyos. (Asegúrese de eliminar cualquier código de ejemplo del editor).

o. Selecciona Guardar seguido de Siguiente.

p. Si lo desea, configure la rotación seguida de Siguiente.

q. Revisa y guarda tu nuevo secreto seleccionando Guardar.

r. Seleccione la pestaña de su navegador en la que tenga abierta la página SES Crear un nuevo punto final de entrada y, a continuación, elija Actualizar lista y, a continuación, seleccione su secreto recién creado en Secret ARN.

6. Seleccione Crear retransmisión SMTP.
7. Puedes ver y administrar los relés SMTP que ya has creado desde la página de retransmisiones SMTP. Si hay una retransmisión SMTP que quieras eliminar, selecciona su botón de radio y, a continuación, selecciona Eliminar.
8. Para editar una retransmisión SMTP, selecciona su nombre. En la página de detalles, puede cambiar el nombre de la retransmisión, el nombre, el puerto y las credenciales de inicio de sesión del servidor SMTP externo. Para ello, pulse el botón de edición o actualización correspondiente y, a continuación, seleccione Guardar cambios.

Configurar Google Workspaces para la retransmisión SMTP entrante (no autenticada)

En el siguiente ejemplo explicativo, se muestra cómo configurar Google Workspaces para que funcione con una retransmisión SMTP entrante (no autenticada) de Mail Manager.

Requisitos previos

- Acceso a la consola de administrador de Google (consola de administrador de Google > Aplicaciones > Google Workspace > Gmail).
- Acceso al servidor de nombres de dominio que aloja los registros MX de los dominios que se utilizarán para configurar Mail Manager.

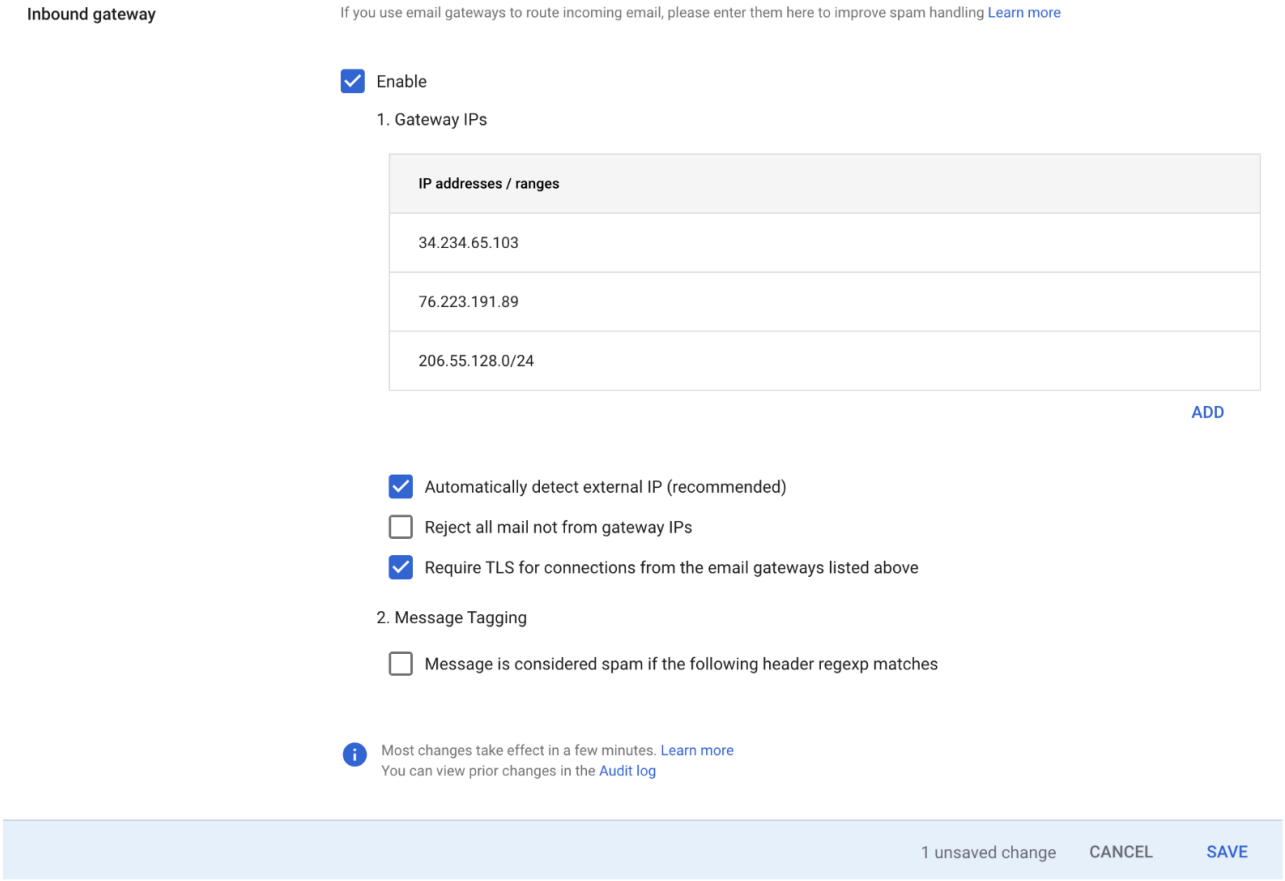
Para configurar Google Workspaces para que funcione con una retransmisión SMTP entrante

- Agrega las direcciones IP de Mail Manager a la configuración de la puerta de enlace entrante

a. En la consola de administración de Google, ve a Aplicaciones > Google Workspace > Gmail.

b. Selecciona Spam, suplantación de identidad y malware y, a continuación, ve a Configuración de la puerta de enlace entrante.

c. Habilita la puerta de enlace entrante y configúrala con los siguientes detalles:



- En las direcciones IP de las puertas de enlace, seleccione Añadir y añada las direcciones IP de los puntos de conexión de entrada específicas de su región en la siguiente tabla:

Región	Rango de IP
EU-West-1/DUB	206,55.133,0/24
EU-Central-1/FRA	206.55.132.0/24
US-Oest-2/PDX	206.55.131.0/24
AP-Northeast-1/NRT	206,55.130,0/24

Región	Rango de IP
US-East-1/IAD	206.55.129.0/24
AP-Soudeste-2/SYD	206.55.128.0/24

- Seleccione Detectar automáticamente la IP externa.
- Selecciona Requerir TLS para las conexiones desde las pasarelas de correo electrónico mencionadas anteriormente.
- Seleccione Guardar en la parte inferior del cuadro de diálogo para guardar la configuración. Una vez guardada, la consola de administración mostrará la puerta de enlace entrante como habilitada.

Configuración de Microsoft Office 365 para la retransmisión SMTP entrante (no autenticada)

En el siguiente ejemplo explicativo, se muestra cómo configurar Microsoft Office 365 para que funcione con una retransmisión SMTP entrante (no autenticada) de Mail Manager.

Requisitos previos

- Acceso al centro de administración de Microsoft Security (centro de administración de Microsoft Security > Correo electrónico y colaboración > Políticas y reglas > Políticas de amenazas).
- Acceso al servidor de nombres de dominio que aloja los registros MX de los dominios que se utilizarán para configurar Mail Manager.

Para configurar Microsoft Office 365 para que funcione con una retransmisión SMTP entrante

1. Agregue las direcciones IP de Mail Manager a la lista de permitidos

    a. En el centro de administración de Microsoft Security, vaya a Correo electrónico y colaboración > Políticas y reglas > Políticas de amenazas.

    b. Seleccione Antispam en Políticas.

    c. Seleccione Política de filtro de conexiones seguido de Editar política de filtro de conexiones.

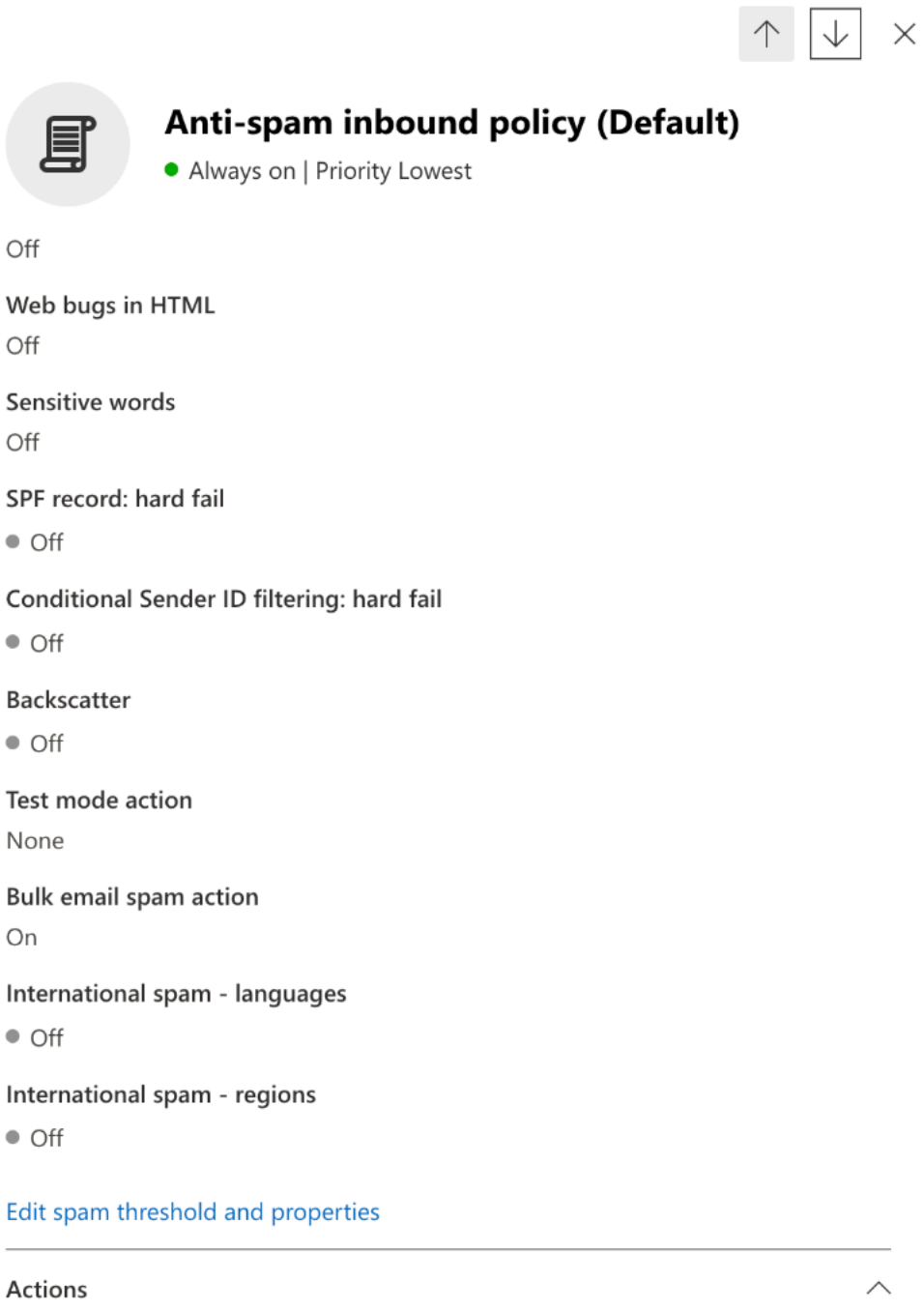
- En el cuadro de diálogo Permitir siempre mensajes de las siguientes direcciones IP o rango de direcciones, añada las IP de los puntos de entrada específicos de su región en la siguiente tabla:

Región	Rango de IP
EU-West-1/DUB	206,55.133,0/24
EU-Central-1/FRA	206.55.132.0/24
US-Oest-2/PDX	206.55.131.0/24
AP-Northeast-1/NRT	206,55.130,0/24
US-East-1/IAD	206.55.129.0/24
AP-Soudeste-2/SYD	206.55.128.0/24

- Seleccione Guardar.

d. Vuelva a la opción Antispam y elija Política antispam entrante.

- En la parte inferior del cuadro de diálogo, selecciona Editar el umbral y las propiedades del correo no deseado:



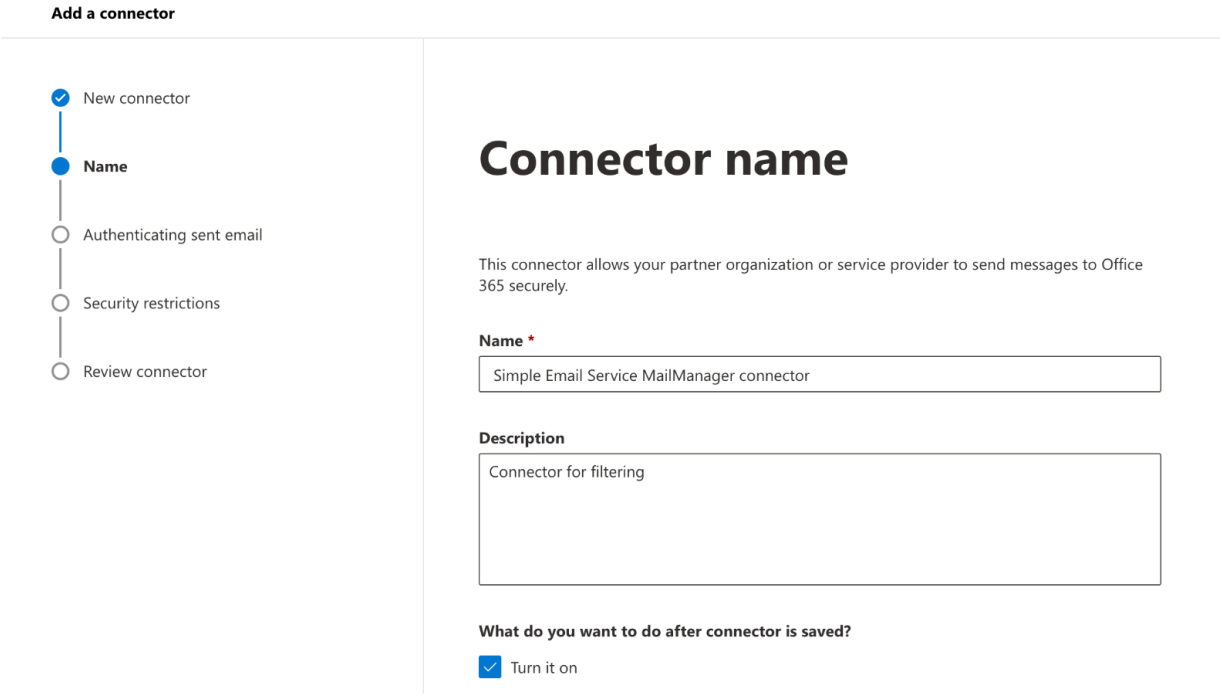
- Desplázate hasta Marcar como spam y asegúrate de que el SPF record: hard fail esté desactivado.
- Seleccione Guardar.

2. Configuración de filtrado mejorada (recomendada)

   Esta opción permitirá a Microsoft Office 365 identificar correctamente la IP de conexión original antes de que SES Mail Manager recibiera el mensaje.

a. Cree un conector entrante

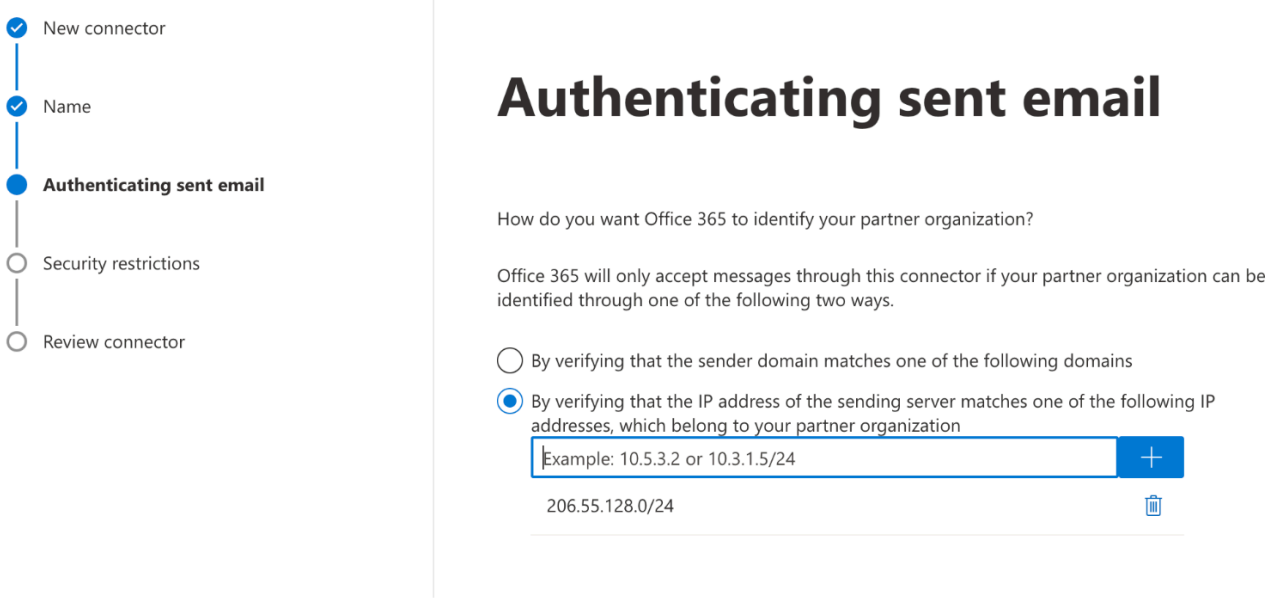
- Inicie sesión en el nuevo centro de administración de Exchange y vaya a Flujo de correo > Conectores.
- Selecciona Añadir un conector.
- En Conexión desde, selecciona Organización asociada y, a continuación, Siguiente.
- Rellene los campos de la siguiente manera:
  - Nombre: conector de Mail Manager de Simple Email Service
  - Descripción: conector para filtrar



- Seleccione Siguiente.
- En Autenticar el correo electrónico enviado, seleccione Verificando que la dirección IP del servidor remitente coincide con una de las siguientes direcciones IP, que pertenecen a su organización asociada, y añada las IP de punto final de entrada específicas de su región en la siguiente tabla:

Región	Rango de IP
EU-West-1/DUB	206,55.133,0/24

Región	Rango de IP
EU-Central-1/FRA	206.55.132.0/24
US-Oest-2/PDX	206.55.131.0/24
AP-Northeast-1/NRT	206,55.130,0/24
US-East-1/IAD	206.55.129.0/24
AP-Soudeste-2/SYD	206.55.128.0/24

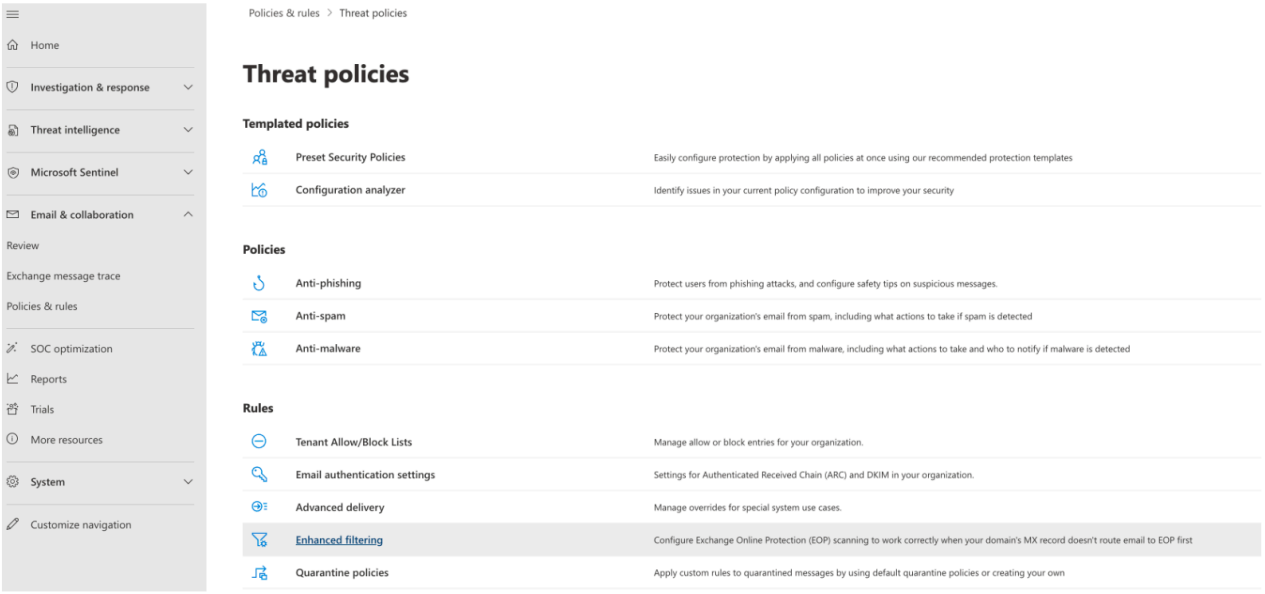


- Seleccione Siguiente.
- En Restricciones de seguridad, acepta la configuración predeterminada Rechazar los mensajes de correo electrónico si no se envían a través de TLS, seguida de Siguiente.
- Revisa la configuración y selecciona Crear conector.

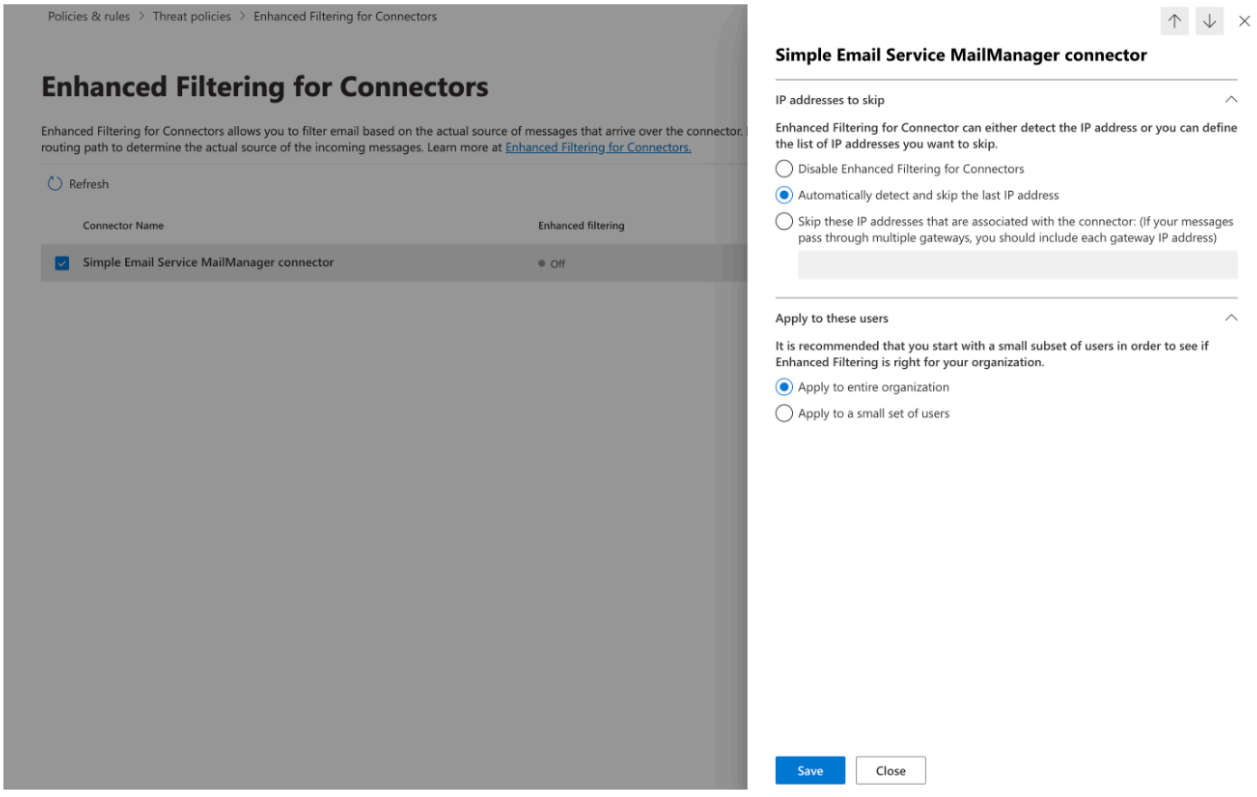
b. Habilita el filtrado mejorado

Ahora que se ha configurado el conector de entrada, tendrá que habilitar la configuración de filtrado mejorada del conector en el centro de administración de Microsoft Security.

- En el centro de administración de Microsoft Security, vaya a Correo electrónico y colaboración > Políticas y reglas > Políticas de amenazas.
- Seleccione Filtrado mejorado en Reglas.



- Seleccione el conector Mail Manager de Simple Email Service que creó anteriormente para editar sus parámetros de configuración.
- Seleccione Detectar automáticamente y omitir la última dirección IP y Aplicar a toda la organización.



- Seleccione Guardar.

Archivado de correo electrónico

El archivado del correo electrónico le permite archivar los tipos de correo electrónico que especifique que lleguen a su punto de acceso, además de encontrar los mensajes archivados mediante un amplio conjunto de filtros de búsqueda avanzada y la posibilidad de exportar los resultados.

El archivado del correo electrónico guarda y protege sus correos electrónicos al almacenar los datos en un almacenamiento persistente y seguro a largo plazo, y le permite buscar y archivar rápidamente el correo electrónico. Permite archivar a tiempo completo a nivel empresarial sin aumentar los requisitos de almacenamiento del servidor de buzones de correo.

Cuando su terminal de entrada recibe correo electrónico, utiliza una política de tráfico para determinar qué correos electrónicos bloquear o permitir. El correo electrónico que permitas entrar pasa a un conjunto de reglas que aplica reglas condicionales para ejecutar las acciones que has definido para tipos específicos de correo electrónico. Una de las acciones de la regla que puedes definir es la acción de archivar: si seleccionas esta acción, el correo electrónico se archivará en el archivo de correo que designes.

Primero debe crear un archivo para poder designarlo en una acción de regla. El procedimiento de la siguiente sección le explicará cómo crear un archivo en la consola de SES.

Uso del archivado de correo electrónico en la consola de Amazon SES

La página de archivado de correo electrónico de la consola de SES consta de cuatro tablas interactivas: Archivo de búsqueda, Historial de búsqueda, Historial de exportaciones y Administración de archivos, que puede utilizar para buscar correo electrónico en sus archivos, exportar los resultados y administrar sus archivos. En los siguientes procedimientos, se proporcionan instrucciones para cada tabla.

Para utilizar la página de archivado de correo electrónico para buscar, exportar y administrar sus archivos

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. En el panel de navegación izquierdo, selecciona Archivado de correo electrónico en Mail Manager.
3. La página de archivado de correo electrónico consta de cuatro tablas: Buscar archivar, Buscar en el historial, Exportar historial y Administrar archivos. Para obtener instrucciones específicas para cada una de estas tablas, selecciona la pestaña correspondiente a continuación:

Search archive

El archivo de búsqueda es una tabla interactiva que te permite buscar y encontrar los mensajes archivados con un amplio filtro y un conjunto de fechas que ofrecen criterios de búsqueda detallados para encontrar cualquier cosa, desde un correo electrónico específico hasta muchos correos que coincidan con una categoría más amplia. Los mensajes que coincidan con tus criterios de búsqueda se pueden descargar de forma individual o se pueden exportar de forma masiva a un depósito de S3.

Para buscar, descargar o exportar correos electrónicos archivados

1. En la página de archivado de correo electrónico, selecciona la pestaña Buscar en el archivo para ver la tabla en el archivo de búsqueda.
2. Haga clic en el campo Archivar y elija un archivo de la lista seguido de Buscar, o bien defina la búsqueda siguiendo estos pasos.
3. Seleccione el campo Intervalo de fechas para ampliar las opciones de intervalo de fechas de la búsqueda:

   - Rango relativo (predeterminado): seleccione el botón de radio que corresponda al número de días deseado o elija un rango personalizado seleccionando una unidad de tiempo y un rango de fechas de hasta 30 días.
   - Rango absoluto: introduzca una fecha de inicio y una fecha de finalización (y una hora si lo desea) hasta 30 días.

> **Note**
>
> - La búsqueda en un archivo está limitada a 30 días cada vez. Por ejemplo, si quieres buscar mensajes del 1 de junio al 31 de julio, tendrás que dividirlos en tres búsquedas de la siguiente manera:
>
>   1. 30 días en junio.
>   2. Los primeros 30 días de julio.
>   3. El día 31 de julio.
>
> - Para las fechas de rango relativo, el último día termina a medianoche. Por ejemplo, si elige Last 7 days (Últimos 7 días), el séptimo día sería ayer y finalizaría a medianoche.

4. (Opcional) Seleccione el campo Filtros para elegir entre los siguientes filtros: De, Para, CC, Línea de asunto y Tiene archivos adjuntos; se aplican las siguientes propiedades:

   - Puede crear hasta 10 filtros.
   - Un filtro se puede editar haciendo clic en él o eliminarlo seleccionando la X.

5. Selecciona Buscar y el correo electrónico archivado que coincida con tus criterios de búsqueda aparecerá en la tabla de resultados de la búsqueda.

   - La columna del identificador del mensaje está oculta de forma predeterminada, pero se puede mostrar seleccionando el icono de engranaje para personalizar la visualización de la tabla.
   - Cada búsqueda que ejecute se guarda automáticamente con un identificador de búsqueda único y aparecerá en la tabla del historial de búsquedas.

6. Para ver el texto de un mensaje junto con la información sobre el sobre y el encabezado, selecciona el botón de radio del mensaje seguido de Ver detalles para abrir la barra lateral de detalles del mensaje.
7. Para crear un archivo local del mensaje, selecciona el botón de opción del mensaje seguido de Descargar mensaje.
8. La búsqueda filtrada se puede guardar en un bucket de Amazon S3 seleccionando Exportar a S3.

   a. Si conoce el URI del bucket de S3 que quiere usar, introdúzcalo en el campo URI de S3; de lo contrario, elija Browse S3 y seleccione un bucket y una carpeta de S3 para usarlos en la página de S3.

   b. (Opcional) Puede cifrar los mensajes exportados introduciendo su propia AWS KMS clave en el campo ARN de la clave KMS o seleccionando Crear nueva clave. De lo contrario, el cifrado se configurará según el método que se utilice en el bucket S3 de destino (aunque no haya ninguno).

   c. Selecciona Exportar y todos los mensajes encontrados en la búsqueda filtrada se guardarán como archivos individuales en la carpeta S3 que hayas seleccionado.

> **Note**
>
> Si bien no hay límite en cuanto al número de mensajes que puede contener tu archivo, los resultados de la búsqueda están limitados a 1000 filas en la tabla de resultados de la búsqueda.

Search history

En esta tabla se muestra un historial de las búsquedas para que pueda restaurar el conjunto de resultados o acceder a conjuntos de filtros complejos creados anteriormente. También puede crear nuevas búsquedas basadas en la búsqueda original editando los filtros y las fechas. Todas las búsquedas nuevas se guardan automáticamente con un identificador de búsqueda único y se muestran en esta tabla.

Para ver tus búsquedas anteriores y trabajar con ellas

1. En la página de archivado del correo electrónico, selecciona la pestaña Historial de búsquedas para ver la tabla del historial de búsquedas, que muestra un historial de todas las búsquedas de correo electrónico archivadas, con las más recientes en la parte superior. Esta tabla carga los datos la primera vez que la visitas. Si cambias de pestaña y vuelves, utiliza el icono de actualización para recuperar los datos más recientes.
2. Haz clic en el campo Archivar y selecciona un archivo de la lista; todas las búsquedas que pertenezcan a ese archivo se rellenarán en la tabla. Puedes ver las búsquedas individuales y hacer más con ellas en los pasos que se indican a continuación.
3. Seleccione el botón de radio de una búsqueda anterior y, a continuación, pulse Ver los resultados de la búsqueda para recuperar los resultados de búsqueda originales. Se abrirá la página del archivo de búsquedas y mostrará el conjunto de filtros y el intervalo de fechas utilizados para la búsqueda original, junto con todos los mensajes encontrados anteriormente según ese criterio. Puede ampliar la búsqueda original de las siguientes maneras:

   - Cree una nueva búsqueda modificando el intervalo de fechas y los filtros y, a continuación, pulse Buscar.
   - Todas las búsquedas nuevas que realices se guardan automáticamente con un identificador de búsqueda único y se muestran en la tabla del historial de búsquedas.

Export history

En esta tabla se incluye un historial de sus exportaciones, lo que permite acceder fácilmente al contenido de la carpeta de exportación en la consola S3.

Para ver sus exportaciones recientes

1. En la página de archivado de correos electrónicos, selecciona la pestaña Historial de exportaciones para ver la tabla del historial de exportaciones, que muestra todas las búsquedas de correo electrónico archivadas que has exportado a un bucket de S3 en los últimos 30 días. Esta tabla carga los datos la primera vez que la visitas. Si cambias de pestaña y vuelves, utiliza el icono de actualización para recuperar los datos más recientes.
2. Si el estado de una exportación es En cola, Preprocesamiento o Procesando, puedes cancelarla pulsando Cancelar.
3. Seleccione un URI de S3 para abrir la carpeta bucket de la exportación en la consola de S3, donde podrá ver los archivos que contiene.

Manage archives

En esta tabla se muestran los archivos en los que tiene opciones para crear uno nuevo, buscar un archivo concreto y ver sus detalles, editar un archivo o eliminar un archivo.

Para crear y administrar archivos

1. En la página de archivado de correo electrónico, seleccione la pestaña Administrar archivos para mostrar la tabla Archivos, que muestra todos los archivos de correo electrónico. Esta tabla carga los datos la primera vez que la visitas. Si cambias de pestaña y vuelves, utiliza el icono de actualización para recuperar los datos más recientes.
2. Para buscar un archivo concreto, empieza a escribir en el campo Archivos.
3. Para ver los detalles de un archivo, seleccione su nombre en la columna Nombre del archivo.
4. Para crear un archivo, seleccione Crear archivo.
    a. Introduce un nombre único en el campo Nombre del archivo.
    b. (Opcional) Seleccione un período de retención en el campo Período de retención para anular el período de retención predeterminado de 180 días.
    c. (Opcional) Puede cifrar el archivo introduciendo su propia AWS KMS clave en el campo ARN de la clave KMS o seleccionando Crear nueva clave.

Elija Crear archivo.

5. Para editar un archivo, seleccione su botón de radio y, a continuación, Editar.

   a. Edite o cambie el nombre en el campo Nombre del archivo.

   b. Cambie el período de retención en el campo Período de retención.

   Seleccione Actualizar archivo.

6. Para eliminar un archivo, seleccione su botón de radio y, a continuación, Eliminar.

   - Escriba `delete` el campo Confirmar seguido de Eliminar.

     El estado del archivo cambiará a Pendiente de eliminación en la tabla Archivos y se eliminará automáticamente después de 30 días.

> **Note**
>
> Si quieres deshacer esta eliminación, crea un ticket para Amazon SES en un plazo de 30 días.

Complementos de correo electrónico

Los complementos de correo electrónico son un conjunto de herramientas de seguridad especializadas de proveedores aprobados por SES que se pueden utilizar para administrar el tipo de correo electrónico que se deja entrar en el punto de acceso y determinar las medidas que se deben tomar con respecto a determinados tipos de correo electrónico. Estas herramientas son soluciones certificadas de seguridad, inteligencia y cumplimiento que están listas para integrarse en su flujo de trabajo de correo electrónico y se pueden activar directamente desde la consola de Mail Manager.

Estos complementos ofrecen la flexibilidad de elegir entre soluciones de seguridad de correo electrónico probadas y adecuadas a sus casos de uso individuales y que se pueden utilizar a un precio reducido, en lugar de adquirir una solución grande y de un solo producto que puede no estar optimizada para ninguna de sus necesidades. Email Add Ons amplía sus funciones principales de inteligencia de amenazas y aplicación de la seguridad en función de la carga de trabajo, por lo que no es necesario adivinar la capacidad necesaria. Estos beneficios le permiten concentrarse

en anticiparse a los problemas de seguridad del correo electrónico y mantener altos estándares de servicio para su organización.

Puede obtener más información sobre cada complemento directamente en la página de complementos de correo electrónico ubicada en la consola de Mail Manager, donde tendrá acceso a las descripciones de los productos, las principales ventajas y la información sobre precios. Una vez que decidas qué complemento quieres usar, solo tienes que suscribirte a él desde la consola de Mail Manager. Una vez suscrito, podrás seleccionarlo como condición de política de tráfico para determinar el correo electrónico permitido en un punto de acceso o como condición establecida por reglas para determinar las medidas que se deben tomar en correos electrónicos específicos. El soporte principal para todos los complementos lo proporciona la consola de AWS Mail Manager, a la que también se puede acceder desde ella.

El procedimiento de la siguiente sección le explicará cómo suscribirse a un complemento de correo electrónico en la consola de Mail Manager.

Suscribirse a los complementos de correo electrónico en la consola de Mail Manager

El siguiente procedimiento le muestra cómo utilizar la página de complementos de correo electrónico de la consola de Mail Manager para suscribirse a un complemento y poder utilizarlo en cualquiera de sus políticas o conjuntos de reglas de tráfico.

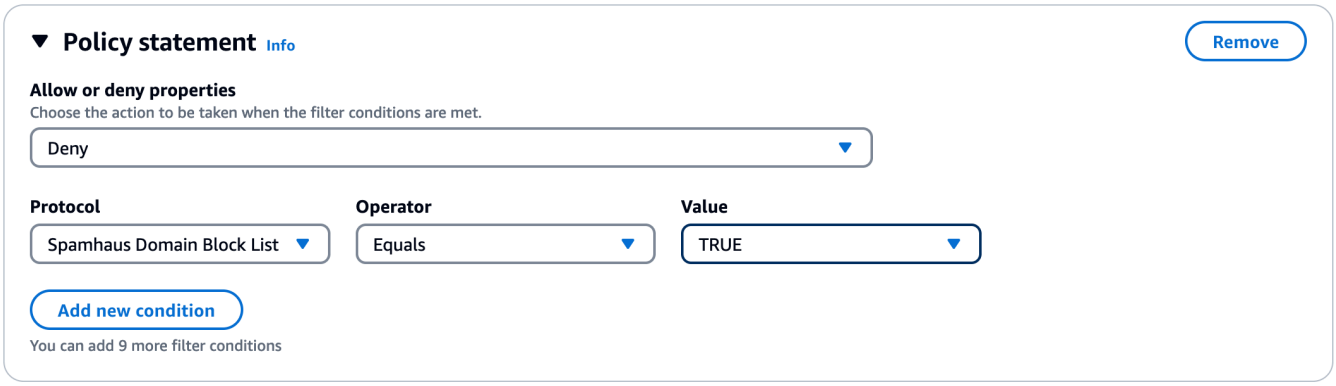
Para suscribirse a un complemento de correo electrónico mediante la consola

1. Inicie sesión en la consola Amazon SES AWS Management Console y ábrala en https://console.aws.amazon.com/ses/.
2. En el panel de navegación izquierdo, selecciona Complementos de correo electrónico en Mail Manager.
3. En la página de complementos por correo electrónico, selecciona el título de cualquier tarjeta de complementos para abrir su página de descripción general, donde podrás obtener más información sobre sus funciones, sus principales ventajas e información sobre precios. Si quieres usar este complemento, selecciona Suscribirse.

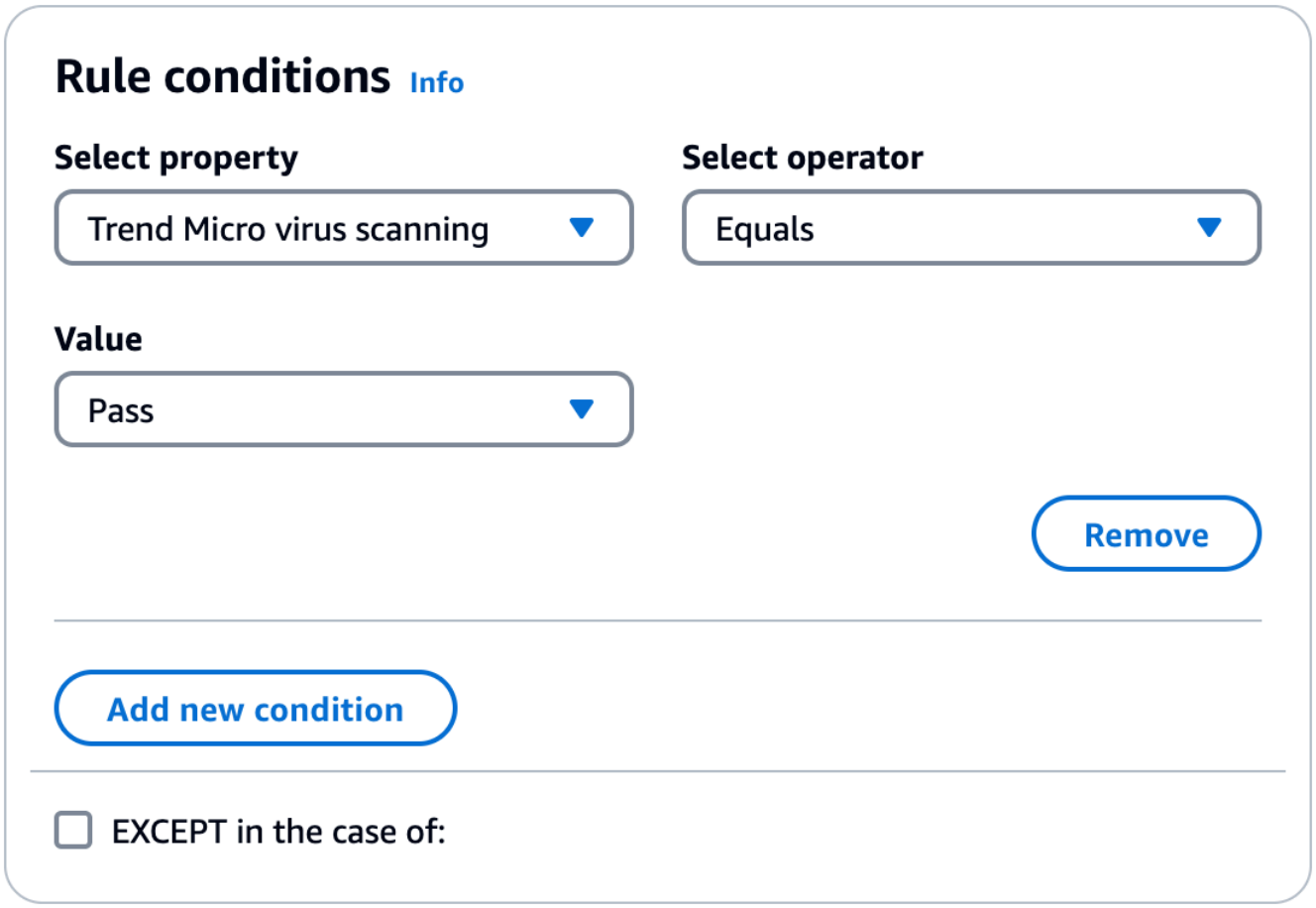
   - Lee los términos y condiciones presentados y marca la casilla Acepto seguida de Suscribirse.
4. Una vez que te hayas suscrito a un complemento, podrás integrarlo en tu flujo de trabajo de correo electrónico seleccionándolo como condición de política de tráfico para denegar o permitir la entrada de correo electrónico a tu punto de acceso, o como condición establecida por reglas

para determinar qué medidas tomar con los mensajes que cumplen los requisitos. Los siguientes ejemplos muestran el uso de un complemento en una condición de declaración de política y en una condición de regla:

- El uso del complemento de la lista de dominios bloqueados de Spamhaus en una condición de declaración de política para bloquear el correo electrónico que llegue a su punto de acceso y que provenga de un dominio incluido en Spamhaus:



- Para obtener más información sobre cómo crear políticas de tráfico y crear condiciones de declaración de políticas con complementos de correo electrónico, consulte. the section called “Creación de políticas y declaraciones de políticas de tráfico (consola)”
- Uso del complemento de detección de virus de Trend Micro en una condición de regla para determinar la acción de la regla para el correo electrónico que supere el análisis de virus:



- Para obtener más información sobre cómo crear conjuntos de reglas y crear condiciones de reglas con complementos de correo electrónico, consultethe section called “Creación de conjuntos de reglas y reglas (consola)”.

5. Para ver los detalles generales o acceder al soporte de cualquier complemento al que esté suscrito, seleccione su nombre en la página de complementos de correo electrónico para abrir su página de información general:

   - En Información general, puedes ver la fecha en la que te suscribiste y el nombre del recurso de Amazon (ARN) de tu complemento.
   - Seleccione la pestaña Support para acceder a los enlaces a AWS Support.

6. Para cancelar la suscripción a un complemento:

   a. Primero debes eliminarlo de cualquiera de tus políticas o conjuntos de reglas de tráfico cuando lo tengas definido en una condición; de lo contrario, los siguientes pasos para cancelar la suscripción fallarán.

b. Seleccione su nombre en la página de complementos de correo electrónico para abrir su página de información general y, a continuación, seleccione Cancelar la suscripción.

c. Escribe `confirm` el campo Confirmar seguido de Cancelar suscripción.

Políticas de permisos para Mail Manager

Las políticas de este capítulo se proporcionan como un punto de referencia único para las políticas necesarias para utilizar todas las diferentes funciones de Mail Manager.

En las páginas de características de Mail Manager, hay enlaces que lo llevarán a la sección correspondiente de esta página que contiene las políticas que necesita para utilizar la función. Seleccione el icono de copia de la política que necesite y péguelo como se indica en la descripción de la función correspondiente.

Las siguientes políticas le otorgan permiso para usar las diferentes funciones incluidas en Amazon SES Mail Manager a través de políticas y AWS Secrets Manager políticas de permisos de recursos. Si es la primera vez que utiliza las políticas de permisos, consulte the section called “Anatomía de las políticas” las políticas de permisos para AWS Secrets Manager.

Políticas de permisos para el punto final de Ingress

Las dos políticas de esta sección son necesarias para crear un punto final de entrada. Para obtener información sobre cómo crear un punto final de entrada y dónde usar estas políticas, consulte. the section called “Crear un punto final de entrada (consola)”

Secrets Manager oculta la política de permisos de recursos para el punto final de entrada

Se requiere la siguiente política de permisos de recursos Secrets Manager secrets para permitir que SES acceda al secreto mediante el recurso de punto final de entrada.

```
{
    "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/*"
                }
            }
        }
    ]
}
```

Política de claves gestionadas por el cliente (CMK) de KMS para el punto final de entrada

La siguiente política de claves administradas por el cliente (CMK) de KMS es necesaria para permitir que SES use su clave mientras usa su secreto.

```
{
    "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/*"
        }
    }
}
```

Políticas de permisos para la retransmisión SMTP

Las dos políticas de esta sección son necesarias para crear una retransmisión SMTP. Para obtener información sobre cómo crear una retransmisión SMTP y dónde usar estas políticas, consulte. the section called “Crear un relé SMTP (consola)”

Secrets Manager secreta la política de permisos de recursos para la retransmisión SMTP

Se requiere la siguiente política de permisos del recurso Secrets Manager secrets para permitir que SES acceda al secreto mediante el recurso de retransmisión SMTP.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Principal": {
                "Service": [
                    "ses.amazonaws.com"
                ]
            },
            "Resource": "*",
            "Condition": {
               "StringEquals": {
                   "aws:SourceAccount": "888888888888"
                },
               "ArnLike": {
                   "aws:SourceArn": "arn:aws:ses:us-east-1:888888888888:mailmanager-
smtp-relay/*"
               }
           }
        }
    ]
}
```

Política de claves administradas por el cliente (CMK) de KMS para la retransmisión SMTP

La siguiente política de claves administradas por el cliente (CMK) de KMS es necesaria para permitir que SES use su clave mientras usa su secreto.

```
{
    "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/*"
                }
            }
        }
    ]
}
```

Políticas de permisos para archivar correos electrónicos

Políticas básicas de archivado e identidad (IAM)

Estas son las políticas de identidad de IAM para autorizar las operaciones de archivado. Es posible que estas políticas por sí solas no sean suficientes para algunas operaciones (consulte Archivar el cifrado en reposo con la CMK de KMS y Archivar la exportación).

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ses:CreateArchive",
                "ses:TagResource"
            ],
            "Resource": [
                "arn:aws:ses:us-east-1:000000000000:mailmanager-archive/*"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:RequestTag/key-name": [
                        "value1",
                        "value2"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ses:ListArchives"
            ],
            "Resource": [
                "arn:aws:ses:us-east-1:000000000000:mailmanager-archive/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ses:GetArchive",
                "ses:DeleteArchive",
                "ses:UpdateArchive"
            ],
            "Resource": [
                "arn:aws:ses:us-east-1:000000000000:mailmanager-archive/MyArchiveID"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ses:ListArchiveSearches"
```

```
            ],
            "Resource": [
                "arn:aws:ses:us-east-1:000000000000:mailmanager-archive/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ses:GetArchiveSearch",
                "ses:GetArchiveSearchResults",
                "ses:StartArchiveSearch",
                "ses:StopArchiveSearch"
            ],
            "Resource": [
                "arn:aws:ses:us-east-1:000000000000:mailmanager-archive/MyArchiveID"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ses:GetArchiveMessage",
                "ses:GetArchiveMessageContent"
            ],
            "Resource": [
                "arn:aws:ses:us-east-1:000000000000:mailmanager-archive/MyArchiveID"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ses:ListArchiveExports"
            ],
            "Resource": [
                "arn:aws:ses:us-east-1:000000000000:mailmanager-archive/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ses:GetArchiveExport",
                "ses:StartArchiveExport",
                "ses:StopArchiveExport"
            ],
            "Resource": [
```

```
                "arn:aws:ses:us-east-1:000000000000:mailmanager-archive/MyArchiveID"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ses:ListTagsForResource",
                "ses:UntagResource"
            ],
            "Resource": [
                "arn:aws:ses:us-east-1:000000000000:mailmanager-archive/MyArchiveID"
            ]
        }
    ]
}
```

Archivar y exportar

Estas son las políticas de identidad de IAM (además de las políticas básicas de archivado anteriores) necesarias para ello. `StartArchiveExport`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::MyDestinationBucketName"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectTagging",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::MyDestinationBucketName/*"
        }
    ]
```

```
}
```

Esta es la política para el segmento de destino.

```
{
    "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**
>
> El archivado no admite claves de condición secundarias confusas (aws:SourceArn, aws:SourceAccount, aws: SourceOrg ID o aws:SourceOrgPaths). Esto se debe a que el archivado del correo electrónico de Mail Manager evita el confuso problema de los adjuntos al comprobar si la identidad que llama tiene permisos de escritura en el segmento de destino

de la exportación mediante sesiones de acceso directo antes de iniciar la exportación propiamente dicha.

Archivar el cifrado en reposo con KMS CMK

Se trata del cifrado en reposo con las políticas de claves administradas por el cliente (CMK) de KMS (además de las políticas básicas de archivado anteriores) necesarias para crear archivos y trabajar con ellos (utilizando cualquier API de archivado).

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "kms:DescribeKey",
            "kms:Decrypt",
            "kms:GenerateDataKey"
        ],
        "Resource": "arn:aws:kms:us-west-2:111122223333:key/MyKmsKeyArnID"
    }
}
```

Esta es la política de claves de KMS necesaria para archivar el correo electrónico.

```
{
    "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": "*"
        }
    ]
}
```

Políticas de permisos y confianza para ejecutar acciones de reglas

La función de ejecución de reglas de SES es una función AWS Identity and Access Management (IAM) que otorga a las reglas un permiso de ejecución para acceder a AWS los servicios y recursos. Antes de crear una regla en un conjunto de reglas, debe crear una función de IAM con una política que permita el acceso a los recursos necesarios AWS . SES asume esta función al ejecutar una acción de regla. Por ejemplo, puede crear una función de ejecución de reglas que tenga permiso para escribir un mensaje de correo electrónico en un bucket de S3 como una acción de regla que se llevará a cabo cuando se cumplan las condiciones de la regla.

Por lo tanto, se requiere la siguiente política de confianza, además de las políticas de permisos individuales de esta sección, para ejecutar las acciones de las reglas Escribir en S3, Entregar en el buzón y Enviar a Internet.

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

```
        },
        "Action": "sts:AssumeRole",
        "Condition": {
          "StringEquals": {
                  "aws:SourceAccount": "888888888888"
          },
          "ArnLike": {
             "aws:SourceArn": "arn:aws:ses:us-east-1:888888888888:mailmanager-rule-set/
*"
          }
        }
      }
    ]
  }
```

Política de permisos para la acción de la regla Escribir en S3

La siguiente política es necesaria para utilizar la acción de regla Escribir en S3, que envía el correo electrónico recibido a un bucket de S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::MyDestinationBucketName/*"
      }
    ]
  }
```

Política de permisos para la acción de regla Entregar en el buzón

La siguiente política es necesaria para utilizar la acción de regla Entregar al buzón, que entrega el correo electrónico recibido a una WorkMail cuenta de Amazon.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": ["workmail:DeliverToMailbox"],
```

```
        "Resource": "arn:aws:workmail:us-
east-1:888888888888:organization/MyWorkMailOrganizationID>"
      }
    ]
  }
```

Política de permisos para la acción de la regla «Enviar a Internet»

La siguiente política es necesaria para utilizar la acción de regla Enviar a Internet, que envía el correo electrónico recibido a un dominio externo.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": ["ses:SendEmail", "ses:SendRawEmail"],
        "Resource": "arn:aws:ses:us-east-1:888888888888:identity/example.com"
      }
    ]
  }
```

Gestión de listas y suscripciones en Amazon Simple Email Service

Puede administrar sus propias listas para envío de correo y suscripciones, así como para supresión de correo electrónico en Amazon SES. Para ayudarle a mantener su reputación como remitente, SES ofrece supresión de nivel de cuenta y de nivel de conjunto de configuración que le impide enviar correos a destinatarios no válidos y perjudicar su reputación como remitente. Como medida adicional contra los rebotes y los reclamos de correo electrónico, SES puede agregar automáticamente enlaces de cancelación de suscripción a todo el correo saliente a través de la gestión de suscripciones.

Cada uno de estos tipos de listas se analiza en detalle en las secciones enumeradas en los temas de este capítulo; sin embargo, aquí se presenta información general de las listas de supresión, ya que existen tres tipos de listas de supresión, así como un cambio clave en la gestión global de listas de supresión. Se sugiere que lea esta información general antes de trabajar con cualquiera de las listas analizadas en este capítulo.

Información general de los tres tipos de listas de supresión

La característica de eliminación de listas de supresión global ya no está orientada al cliente y ya no interactuará con ella para administrar las listas de supresión. La lista de supresión global funciona y es administrada en segundo plano por SES. Como cliente, ahora tiene a su disposición listas de supresión de nivel de cuenta y listas de supresión a nivel de conjunto de configuración que le ofrecen un control más personalizado sobre cómo maneja la supresión de correo electrónico de su propia cuenta.

A continuación se explican los diferentes tipos de listas de supresión, su alcance y las ventajas que ofrecen. Los tres tipos de listas de supresión que se utilizan en Amazon SES son los siguientes:

- Lista de supresión global: propiedad y administración a cargo de SES para proteger la reputación de las direcciones del grupo de IP compartidas de SES.
- Lista de supresión de nivel de cuenta: propiedad y administración a cargo del cliente para proteger la reputación de su cuenta, reemplaza la lista de supresión global.
- Supresión de nivel de conjunto de configuración: propiedad y administración a cargo del cliente para proporcionar un control condicional o detallado sobre la gestión de listas de supresión, invalida la lista de supresión de nivel de cuenta.

La lista de supresión global era el único tipo de lista de supresión hasta que se introdujo la supresión de nivel de cuenta y conjunto de configuración en la nueva consola de Amazon SES y API v2. La propiedad y administración de la lista de supresión global está a cargo de SES para proteger la reputación de las direcciones del grupo de IP compartidas de SES. Esto es necesario porque todos los clientes de SES comparten el mismo grupo de direcciones IP (a menos que tengan IP dedicadas), y es importante que SES se asegure de que los clientes no envíen spam ni nada que afecte negativamente a la reputación de esas direcciones IP en el grupo de IP compartidas de SES. Si bien usted ya no interactúa directamente con la lista de supresión global, la misma sigue funcionando en segundo plano y los principios generales de cómo funciona la lista de supresión global también se pueden aplicar para explicar los principios generales de cómo funcionan los otros tipos de listas de supresión. Consulte Lista de supresión global de Amazon SES.

> **Note**
>
> El formulario de solicitud de eliminación de listas de supresión global ya no se encuentra en la consola de Amazon SES porque la lista de supresión a nivel de cuenta lo ha sustituido, con motivo de todas las ventajas que se explican en esta sección.

Se introdujo la lista de supresión de nivel de cuenta para que los clientes puedan crear y controlar sus propias listas de supresión y reputación, por lo que la lista de supresión de nivel de cuenta se aplica únicamente a su cuenta. La interfaz de lista de supresión de nivel de cuenta de la nueva consola proporciona una forma sencilla de administrar las direcciones de la lista de supresión de nivel de cuenta, incluidas acciones masivas para agregar o quitar direcciones. Si una dirección está en la lista global de supresión, pero no en su lista de supresión de nivel de cuenta (lo que significa que quiere realizar envíos a esa dirección), y así lo hace, Amazon SES seguirá intentando realizar la entrega, pero si rebota, el rebote afectará su reputación, pero nadie más recibirá rebotes porque no podrán realizar envíos a esa dirección de correo electrónico si no están utilizando su propia lista de supresión de nivel de cuenta; por lo tanto, la lista de supresión de nivel de cuenta anula la lista de supresión global únicamente para su cuenta. Consulte Uso de la lista de supresión de nivel de cuenta de Amazon SES.

La supresión de nivel de conjunto de configuración le permite configurar personalizaciones de supresión e invalidaciones en la lista de supresión de nivel de cuenta a través del uso de conjuntos de configuración creados específicamente para diferentes escenarios de envío de correo electrónico. Por ejemplo, si la lista de supresión de nivel de cuenta está configurada para agregar direcciones de rebote y reclamación, pero tiene un determinado grupo demográfico de correo electrónico definido en un conjunto de configuración para el que solo le interesa agregar direcciones de reclamación,

lo lograría habilitando las invalidaciones de supresión del conjunto de configuración para que las direcciones de correo electrónico se agreguen a la lista de supresión de nivel de cuenta solo para reclamaciones (no rebotes y reclamaciones como se establece en la lista de supresión de nivel de cuenta) del correo electrónico enviado con este conjunto de configuración. Con la supresión de nivel de conjunto de configuración, existen diferentes niveles de invalidación de la supresión de nivel de cuenta, incluso no utilizar ninguna supresión. Consulte Uso de la supresión de nivel de conjunto de configuración para invalidar la lista de supresión de nivel de cuenta.

Lista de supresión global de Amazon SES

Amazon SES mantiene una lista de supresión global interna que es administrada en segundo plano por SES. Cuando un cliente de SES envía un correo electrónico que produce un rechazo permanente, SES agrega la dirección de correo electrónico que produjo el rebote a una lista de supresión global. La lista de supresión global es global en el sentido de que se aplica a todos los clientes de SES. En otras palabras, si otro cliente intenta enviar un correo electrónico a una dirección incluida en la lista de supresión global, SES acepta el mensaje pero no lo envía, ya que la dirección de correo electrónico está suprimida.

La característica de solicitud de eliminación de direcciones de correo electrónico de listas de supresión global ya no está orientada al cliente y ya no interactuará con ella para administrar las listas de supresión. Para sustituir esta funcionalidad, Amazon SES ofrece ahora una nueva forma de administrar las listas de supresión poniendo a disposición listas de supresión a nivel de cuenta y listas de supresión a nivel de conjunto de configuración que ofrecen un control más personalizado sobre cómo maneja la supresión de correo electrónico en su propia cuenta. Para obtener más información, consulte Uso de la lista de supresión de nivel de cuenta de Amazon SES y Uso de la supresión de nivel de conjunto de configuración para invalidar la lista de supresión de nivel de cuenta.

> **Important**
>
> El formulario de solicitud de supresión de direcciones de correo electrónico de la lista de supresión global ya no se encuentra en la consola de Amazon SES porque la lista de supresión a nivel de cuenta la ha sustituido. Para obtener más información acerca de cómo utilizar la lista de supresión a nivel de cuenta, consulte Uso de la lista de supresión de nivel de cuenta de Amazon SES.

Consideraciones sobre la lista de supresión global

Factores clave de la lista de supresión global:

- La lista de supresión global es administrada en segundo plano por SES; no puede interactuar directamente con ella; sin embargo, puede anularla al utilizar su propia lista de supresión a nivel de cuenta.
- La lista de supresión global está habilitada de forma predeterminada para todas las cuentas de SES. No se puede desactivar.
- Como SES aplica la lista de supresión global a todos los clientes, no puede consultar la lista de supresión global ni agregar direcciones manualmente.
- Cuando una dirección de correo electrónico produce un rechazo permanente, SES agrega la dirección a la lista de supresión global por un breve periodo. Después de ese periodo, SES elimina la dirección de la lista. Si la dirección produce otro rechazo permanente, SES la agrega de nuevo a la lista de supresión global durante un periodo más largo y la elimina al final de ese periodo. La cantidad de tiempo que una dirección permanece en la lista de supresión global aumenta cada vez que la dirección produce un rechazo permanente. Una dirección puede permanecer en la lista de supresión global durante un periodo máximo de 14 días.
- Si intenta enviar un mensaje a una dirección incluida en la lista de supresión global, SES acepta el mensaje, pero no lo envía. SES genera una notificación de rebote con el valor `bounceType` de `Permanent` y el valor `bounceSubType` de `Suppressed`. Recibir este tipo de notificación de rebote es la única forma de saber si una dirección está en la lista de supresión global. No se puede consultar la lista de supresión global.
- SES contabiliza los mensajes que envía a las direcciones de la lista de supresión global en el cálculo de la tasa de rebotes de su cuenta y en su cuota de envío diaria.
- Al igual que en el caso de una dirección de correo electrónico que produce un rebote permanente, debe eliminar de su lista de correo las direcciones que provocan un rebote de lista de supresión a menos que esté absolutamente seguro de que la dirección es válida.
- Los rebotes de lista de supresión se incluyen en la tasa de rebotes de su cuenta. Si la tasa de rebotes es demasiado alta, su cuenta podría someterse a un proceso de revisión o podría suspenderse la capacidad de su cuenta para enviar correo electrónico.

> **Note**
>
> Es importante entender cómo las tres listas de supresión de SES están interrelacionadas y su jerarquía; para ello, consulte Información general de los tres tipos de listas de supresión.

Uso de la lista de supresión de nivel de cuenta de Amazon SES

Se introdujo la lista de supresión de nivel de cuenta de Amazon SES para que los clientes puedan crear y controlar sus propias listas de supresión y reputación, por lo que la lista de supresión de nivel de cuenta se aplica únicamente a la cuenta. La interfaz de lista de supresión de nivel de cuenta de la consola de SES proporciona una forma sencilla de administrar las direcciones de la lista de supresión de nivel de cuenta, incluidas acciones masivas para agregar o quitar direcciones.

SES incluye una lista de supresión de nivel de cuenta que se aplica a la Cuenta de AWS en la Región de AWS actual. Puede agregar o eliminar direcciones, ya sea de manera individual o en bloque, en la lista de supresión de nivel de cuenta mediante la API v2 de SES o la consola.

> **Note**
>
> Para agregar o eliminar direcciones en bloque, debe tener acceso de producción. Para obtener más información sobre el entorno de pruebas, consulte Solicitar acceso a la producción (salir del entorno de pruebas de Amazon SES).

Consideraciones de la lista de supresión de nivel de cuenta de Amazon SES

Debe tener en cuenta los siguientes factores cuando utilice la lista de supresión de nivel de cuenta:

- Si comenzó a usar Amazon SES después del 25 de noviembre de 2019, su cuenta utiliza la lista de supresión de nivel de cuenta de forma predeterminada, tanto para los rebotes como para los reclamos. Si comenzó a usar SES antes de esta fecha, debe habilitar esta característica mediante la operación `PutAccountSuppressionAttributes` en la API de SES.
- Si intenta enviar un mensaje a una dirección incluida en la lista de supresión en el nivel de la cuenta que tiene un motivo de supresión que coincide con el motivo de supresión elegido para la configuración de la supresión en el nivel de la cuenta, SES acepta el mensaje, pero no lo envía;

sin embargo, si no coincide, SES lo enviará. Para ayudar a aclarar esto, se proporcionan los siguientes ejemplos:

  - Si ha establecido la configuración de supresión en el nivel de la cuenta con el motivo de supresión de solo rebotes, SES no intentará realizar envíos a direcciones en la lista de supresión en el nivel de la cuenta cuyo motivo de supresión sea rebote.
  - Si ha establecido la configuración de supresión en el nivel de la cuenta con el motivo de supresión de rebotes y reclamaciones, SES no intentará realizar envíos a direcciones en la lista de supresión en el nivel de la cuenta cuyo motivo de supresión sea rebote o reclamación.
  - Si ha establecido la configuración de supresión en el nivel de la cuenta con el motivo de supresión de solo rebotes, SES intentará realizar envíos a direcciones en la lista de supresión en el nivel de la cuenta cuyo motivo de supresión sea reclamación (porque si es el caso, no coinciden).
- SES no contabiliza los mensajes que envía a las direcciones de la lista de supresión de nivel de cuenta en el cálculo de las tasas de rebotes o quejas de la cuenta.
- Si una dirección está en la lista de supresión global, pero no en la lista de supresión en el nivel de la cuenta, (lo que significa que desea enviarla), y la envía a esta, SES todavía intentará la entrega; sin embargo, si rebota, lo tendrá en cuenta al calcular la tasa de devolución de la cuenta y la cuota de envío diaria.
- SES contabiliza los mensajes que envía a las direcciones de la lista de supresión de nivel de cuenta en el cálculo de la cuota de envío diaria.
- Las direcciones de correo electrónico de la lista de supresión de nivel de cuenta permanecen allí hasta que las elimine.
- Si la capacidad de la cuenta para enviar correo electrónico está suspendida, SES elimina de forma automática las direcciones de la lista de supresión correspondiente a la cuenta después de 90 días. Si la capacidad de su cuenta para enviar correo electrónico se restaura antes de que finalice este periodo de 90 días, las direcciones incluidas en la lista no se eliminan.
- Gmail no proporciona datos de reclamaciones a SES. Si un destinatario utiliza el botón Spam del cliente web de Gmail para informar de que ha recibido un mensaje suyo como spam, no se agregará a la lista de supresión de nivel de cuenta.
- Puede habilitar la lista de supresión de nivel de cuenta si la cuenta está en el entorno aislado de SES. Sin embargo, no puede utilizar la operación PutSuppressedDestination ni CreateImportJob hasta que su cuenta se elimine del entorno de pruebas. Para obtener más información sobre el entorno de pruebas, consulte Solicitar acceso a la producción (salir del entorno de pruebas de Amazon SES).

- Solo las devoluciones permanentes se agregan a la lista de supresión a nivel de la cuenta. Para obtener información acerca de las devoluciones permanentes y devoluciones temporales, consulte the section called “Después de que Amazon SES envíe un correo electrónico”.
- Cuando utiliza la lista de supresión en el nivel de la cuenta, SES también agrega direcciones que producen devoluciones permanentes a la lista de supresión global.

Habilitar la lista de supresión de nivel de cuenta de Amazon SES

Puede utilizar la operación PutAccountSuppressionAttributes de la API v2 de Amazon SES para habilitar y configurar la lista de supresión de nivel de cuenta. Para establecer esta configuración de forma rápida y fácil, utilice la AWS CLI. Para obtener más información sobre cómo instalar y configurar la AWS CLI, consulte la Guía del usuario de la AWS Command Line Interface.

Para configurar la lista de supresión de nivel de cuenta mediante la AWS CLI

- En la línea de comandos, escriba el comando siguiente.

  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
  ```

  Para habilitar la lista de supresión de nivel de cuenta, debe especificar al menos un motivo para el parámetro `suppressed-reasons`. Puede especificar `BOUNCE` o `COMPLAINT`, o bien ambos, como se muestra en el ejemplo anterior.

Para configurar la lista de supresión de nivel de cuenta mediante la consola de SES:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Suppression list (Lista de supresión).

3. En el panel Account-level settings (Configuración de nivel de cuenta), seleccione Edit (Editar).
4. En Suppression list (Lista de supresión), marque la casilla Enabled (Habilitado).
5. En Suppression reasons (Motivos de supresión), seleccione uno de los motivos por los que se deben agregar de forma automática las direcciones de correo electrónico de los destinatarios a su lista de supresión de nivel de cuenta.
6. Elija Guardar cambios.

Activación de la lista de supresión de nivel de cuenta de Amazon SES para un conjunto de configuración

También puede configurar la supresión de nivel de cuenta de Amazon SES para que solo se aplique a conjuntos de configuración específicos. Cuando lo haga, las direcciones solo se añaden a la lista de supresión si especificó el conjunto de configuración al enviar el correo electrónico que causó el evento de rebote o reclamación.

> **Note**
>
> En el procedimiento siguiente se presupone que ya ha instalado la AWS CLI. Para obtener más información sobre cómo instalar y configurar la AWS CLI, consulte la Guía del usuario de la AWS Command Line Interface.

Para configurar la lista de supresión de nivel de cuenta para un conjunto de configuración mediante la AWS CLI

- En la línea de comandos, escriba el comando siguiente.

  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
```

En el ejemplo anterior, reemplace *configSet* por el nombre del conjunto de configuración que debe utilizar la lista de supresión de nivel de cuenta.

Para configurar la lista de supresión de nivel de cuenta para un conjunto de configuración mediante la consola de SES:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Configuration sets (Conjuntos de configuración).
3. En Configuration sets (Conjuntos de configuración), elija el nombre del conjunto de configuración que desea configurar con supresión personalizada.
4. En el panel Suppression list options (Opciones de lista de supresión), elija Edit (Editar).
5. La sección Suppression list options (Opciones de lista de supresión) proporciona un conjunto de decisiones para definir la supresión personalizada, a partir de la opción de utilizar este conjunto de configuración para anular la supresión de nivel de cuenta. El mapa lógico de supresión de nivel de conjunto de configuración le ayudará a comprender los efectos de las combinaciones de anulación. Estas selecciones de anulaciones de varios niveles se pueden combinar para implementar tres niveles diferentes de supresión:

   a. Use account-level suppression (Utilizar supresión de nivel de cuenta): no anular la supresión de nivel de cuenta y no implementar ninguna supresión de nivel de conjunto de configuración; básicamente, cualquier correo electrónico enviado con este conjunto de configuración solo utilizará la supresión de nivel de cuenta. Para ello:

      - En Suppression list settings (Configuración de lista de supresión), desmarque la casilla Override account level settings (Anular la configuración de nivel de cuenta).

   b. Do not use any suppression (No utilizar ninguna supresión): anular la supresión de nivel de cuenta sin habilitar ninguna supresión de nivel de conjunto de configuración; esto significa que cualquier correo electrónico enviado con este conjunto de configuración no utilizará ninguna supresión de nivel de cuenta; en otras palabras, se cancelará toda supresión. Para ello:

i. En Suppression list settings (Configuración de lista de supresión), marque la casilla Override account level settings (Anular la configuración de nivel de cuenta).

ii. En Suppression list (Lista de supresión), desmarque la casilla Enabled (Habilitado).

c. Use configuration set-level suppression (Utilizar supresión de nivel de conjunto de configuración): anular la supresión de nivel de cuenta con configuraciones de la lista de supresión personalizada definida en este conjunto de configuración; esto significa que cualquier correo electrónico enviado con este conjunto de configuración solo utilizará su propia configuración de supresión e ignorará cualquier configuración de supresión de nivel de cuenta. Para ello:

i. En Suppression list settings (Configuración de lista de supresión), marque la casilla Override account level settings (Anular la configuración de nivel de cuenta).

ii. En Suppression list (Lista de supresión), marque Enabled (Habilitado).

iii. En Specify the reason(s)... [Especificar el motivo (s)...], seleccione uno de los motivos de supresión que utilizará este conjunto de configuración.

6. Elija Guardar cambios.

Agregar direcciones de correo electrónico individuales a la lista de supresión a nivel de cuenta de Amazon SES

Puede agregar direcciones individuales a la lista de supresión del nivel de cuenta de Amazon SES mediante la operación PutSuppressedDestination de la API v2 de SES. No hay límite para el número de direcciones que puede agregar a la lista de supresión de nivel de cuenta.

> **Note**
>
> En el procedimiento siguiente se presupone que ya ha instalado la AWS CLI. Para obtener más información sobre cómo instalar y configurar la AWS CLI, consulte la Guía del usuario de la AWS Command Line Interface.

Para agregar direcciones individuales a la lista de supresión de nivel de cuenta mediante la AWS CLI

- En la línea de comandos, escriba el comando siguiente.

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
```

En el ejemplo anterior, reemplace *recipient@example.com* por la dirección de correo electrónico que desea agregar a la lista de supresión de nivel de cuenta y *BOUNCE* por el motivo por el que agrega la dirección a la lista de supresión (los valores aceptables son `BOUNCE` y `COMPLAINT`).

Para agregar direcciones individuales a la lista de supresión de nivel de cuenta mediante la consola de SES:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Suppression list (Lista de supresión).
3. En el panel Suppression list (Lista de supresión), seleccione Add email address (Agregar dirección de correo electrónico).
4. Escriba una dirección de correo electrónico en el campo Email address (Dirección de correo electrónico) y seleccione un motivo en Suppression reason (Motivo de supresión); si tiene que escribir más direcciones, elija Enter another address (Ingresar otra dirección) y repita la operación para cada una de ellas.
5. Cuando termine de ingresar las direcciones, revise los datos para verificar que sean correctos. Si decide que alguna de las direcciones ingresadas no debería formar parte de este envío, elija el botón Remove (Eliminar).
6. Elija Save changes (Guardar cambios) para agregar las direcciones de correo electrónico ingresadas a su lista de supresión de nivel de cuenta.

Agregar direcciones de correo electrónico en bloque a la lista de supresión de nivel de cuenta de Amazon SES

Puede agregar direcciones en bloque si carga primero su lista de contactos en un objeto de Amazon S3 seguido de la operación CreateImportJob en la API v2 de Amazon SES.

> **Note**
>
> - No hay límite para el número de direcciones que puede agregar a la lista de supresión de nivel de cuenta, pero hay un límite de adición en bloque de 100 000 direcciones en un objeto de Simple Storage Service (Amazon S3) por llamada a la API.
> - Si su origen de datos es un bucket de S3, debe existir en la misma región a la que se está importando.

Para agregar direcciones de correo electrónico en bloque a su lista de supresión de nivel de cuenta, realice los pasos siguientes.

- Cargue su lista de direcciones en un objeto de Amazon S3 en formato CSV o JSON.

  Ejemplo de formato CSV para agregar direcciones:

  ```
  recipient1@example.com,BOUNCE

  recipient2@example.com,COMPLAINT
  ```

  Solo se admiten archivos JSON delimitados por saltos de línea. En este formato, cada línea es un objeto JSON completo que contiene una definición de dirección individual.

  Ejemplo de formato JSON para agregar direcciones:

  ```
  {"emailAddress":"recipient1@example.com","reason":"BOUNCE"}

  {"emailAddress":"recipient2@example.com","reason":"COMPLAINT"}
  ```

  En el ejemplo anterior, reemplace *recipient1@example.com* y *recipient2@example.com* por las direcciones de correo electrónico que desea agregar de la lista de supresión de nivel de cuenta. Las razones aceptables por las que agrega las direcciones a la lista de supresión son *BOUNCE* y *COMPLAINT*.

- Conceda permiso a SES para leer el objeto de Amazon S3.

  Cuando se aplica a un bucket de Amazon S3, la siguiente política otorga permiso a SES para leer dicho bucket. Para obtener más información acerca de la asociación de políticas a buckets de Amazon S3, consulte Uso de políticas de bucket y políticas de usuario en la Guía del usuario de Amazon Simple Storage Service.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSESGet",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::BUCKET-NAME/OBJECT-NAME",
            "Condition": {
                "StringEquals": {
                    "aws:Referer": "AWSACCOUNTID"
                }
            }
        }
    ]
}
```

- Otorgue permiso a SES para utilizar su clave de AWS KMS.

  Si el objeto de Amazon S3 está cifrado con una clave de AWS KMS, debe conceder permiso a Amazon SES para que use la clave de AWS KMS. SES solo puede obtener el permiso de una clave administrada por el cliente, no de una clave de KMS predeterminada. Debe otorgar permiso a SES para utilizar la clave administrada por el cliente. Para ello, agregue una instrucción a la política de la clave.

  Pegue la siguiente instrucción de política en la política de claves para permitir que SES utilice su clave administrada por el cliente.

```
{
   "Sid": "AllowSESToDecrypt",
   "Effect": "Allow",
   "Principal": {
```

```
        "Service":"ses.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
    ],
    "Resource": "*"
}
```

- Utilice la operación CreateImportJob en la API v2 de SES.

> **Note**
>
> En el ejemplo siguiente se presupone que ya ha instalado AWS CLI. Para obtener más información sobre cómo instalar y configurar la AWS CLI, consulte la Guía del usuario de la AWS Command Line Interface.

En la línea de comandos, escriba el comando siguiente: Reemplace *s3bucket* por el nombre de un bucket de Amazon S3 y *s3object* por el nombre de un objeto de Amazon S3.

```
aws sesv2 create-import-job --import-destination
 SuppressionListDestination={SuppressionListImportAction=PUT} --import-data-source
 S3Url=s3://s3bucket/s3object,DataFormat=CSV
```

Para agregar direcciones en bloque a la lista de supresión de nivel de cuenta mediante la consola de SES:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Suppression list (Lista de supresión).
3. En la tabla Suppression list (Lista de supresión), expanda el botón Bulk actions (Acciones masivas) y seleccione Add email addresses in bulk (Agregar direcciones de correo electrónico en forma masiva).
4. En Bulk action specifications (Especificaciones de acción masiva), seleccione entre: (a)Choose file from S3 bucket (Elegir un archivo del bucket de S3) o b)Import from file (Importar desde archivo); se establecen procedimientos para cada método de importación:

a. Choose file from S3 bucket (Elegir un archivo del bucket de S3); si el archivo de origen ya se ha almacenado en un bucket de Amazon S3:

   i. Si conoce el URI del bucket de Amazon S3 que desea utilizar, ingréselo en el campo Amazon S3 URI (URI de Amazon S3); de lo contrario, elija Browse S3 (Examinar S3):

      A. En Buckets (Buckets), elija el nombre del bucket de S3.

      B. En Objects (Objetos), seleccione el nombre del archivo y, a continuación, seleccione Choose (Elegir), esto lo redirigirá a Bulk action specifications (Especificaciones de acción masiva).

      C. (Opcional) Si desea dirigirse a la consola de Amazon S3 para ver detalles sobre su objeto de S3, elija View (Vista).

   ii. En File format (Formato de archivo), seleccione el formato del archivo que ha elegido importar de su bucket de Amazon S3.

   iii. Elija Add email addresses (Agregar direcciones de correo electrónico) para iniciar la importación de direcciones de su archivo; aparecerá una tabla debajo de la pestaña Bulk actions (Acciones masivas).

b. Import from file (Importar desde archivo), si tiene un archivo de origen local para cargar en un bucket de Amazon S3 nuevo o existente:

   i. En Import source file (Importar archivo de origen), seleccione Choose file (Elegir archivo).

   ii. Seleccione el archivo JSON o CSV en el explorador de archivos y elija Open (Abrir), verá el nombre, el tamaño y la fecha de su archivo debajo del botón Choose file (Elegir archivo).

   iii. Expanda Amazon S3 bucket (Bucket de Amazon S3) y seleccione el bucket de S3.

      - Para cargar el archivo en un bucket nuevo, elija Create S3 bucket (Crear bucket de S3), escriba un nombre en el campo Bucket name (Nombre del bucket) y elija Create bucket (Crear bucket).

   iv. Elija Add email addresses (Agregar direcciones de correo electrónico) para iniciar la importación de direcciones de su archivo; aparecerá una tabla debajo de la pestaña Bulk actions (Acciones masivas).

5. Independientemente del método de importación que haya utilizado, su ID de trabajo aparecerá en Bucket name (Acciones masivas), junto con el tipo de importación, el estado y la fecha; para ver los detalles del trabajo, seleccione el ID del trabajo.
6. Seleccione la pestaña Supression list (Lista de supresión) y se mostrarán todas las direcciones de correo electrónico importadas correctamente, junto con el motivo de supresión y la fecha; están disponibles las siguientes opciones:

    a. Seleccione una dirección de correo electrónico o marque su casilla de verificación correspondiente y elija View report (Ver informe) para ver los detalles. (Si se trata de una dirección que se ha agregado en forma automática a su lista de supresión debido a un rebote o reclamo, se mostrará información sobre el evento de valoración que provocó que se agregue, incluidos detalles sobre el mensaje de correo electrónico que produjo el evento desencadenador).

    b. Marque la casilla de verificación correspondiente de una o más direcciones de correo electrónico que desea eliminar de la lista de supresión de cuenta y elija Remove (Eliminar).

Ver una lista de las direcciones que están en la lista de supresión de nivel de cuenta de Amazon SES

Puede ver una lista de todas las direcciones de correo electrónico que están en la lista de supresión de nivel de cuenta de la cuenta mediante la operación ListSuppressedDestinations en la API v2 de SES.

> **Note**
>
> En el procedimiento siguiente se presupone que ya ha instalado la AWS CLI. Para obtener más información sobre cómo instalar y configurar la AWS CLI, consulte la Guía del usuario de la AWS Command Line Interface.

Para ver una lista de todas las direcciones de correo electrónico que están en la lista de supresión de nivel de cuenta

- En la línea de comandos, escriba el comando siguiente.

```
aws sesv2 list-suppressed-destinations
```

El comando anterior devuelve todas las direcciones de correo electrónico que están en la lista de supresión de nivel de cuenta de la cuenta. La salida se parece al siguiente ejemplo:

```
{
    "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"
        }
    ]
}
```

- Nota: Si su salida incluye un campo “NextToken” con un valor de cadena, indica que hay direcciones de correo electrónico adicionales en la lista de supresión de su cuenta. Para ver direcciones suprimidas adicionales, emita otra solicitud a`ListSuppressedDestinations` y pase el valor de cadena devuelto en el parámetro `--next-token` así:

  ```
  aws sesv2 list-suppressed-destinations --next-token string
  ```

  En el comando anterior, sustituya *`string`* con el valor de NextToken devuelto.

  Para obtener más información, consulte Cómo mostrar más de 1000 direcciones de correo electrónico de la lista de supresión en el nivel de la cuenta.

Puede usar la opción `StartDate` para mostrar únicamente las direcciones de correo electrónico que se añadieron a la lista después de una fecha determinada.

Para ver una lista de las direcciones que se agregaron a la lista de supresión de nivel de cuenta después de una fecha específica

- En la línea de comandos, escriba el comando siguiente.

```
aws sesv2 list-suppressed-destinations --start-date 1604394130
```

  En el comando anterior, sustituya *1604394130* por la marca de tiempo Unix de la fecha de inicio.

También puede usar la opción `EndDate` para mostrar únicamente las direcciones de correo electrónico que se añadieron a la lista antes de una fecha determinada.

Para ver una lista de las direcciones que se agregaron a la lista de supresión de nivel de cuenta antes de una fecha específica

- En la línea de comandos, escriba el comando siguiente.

```
aws sesv2 list-suppressed-destinations --end-date 1611126000
```

  En el comando anterior, sustituya *1611126000* por la marca de tiempo Unix de la fecha de finalización.

En la línea de comandos de Linux, macOS o Unix, también puede emplear la utilidad `grep` integrada para buscar direcciones o dominios específicos.

Para buscar una dirección específica en la lista de supresión de nivel de cuenta

- En la línea de comandos, escriba el comando siguiente.

```
aws sesv2 list-suppressed-destinations | grep -A2 'example.com'
```

  En el comando anterior, sustituya *example.com* por la cadena de texto (como la dirección o el dominio) que desea buscar.

Para ver una lista de todas las direcciones de correo electrónico que están en la lista de supresión de nivel de cuenta con la consola de SES:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Suppression list (Lista de supresión).
3. En el panel Supression list (Lista de supresión), se mostrarán todas las direcciones de correo electrónico en su lista de supresión de nivel de cuenta, junto con el motivo de supresión y la fecha; están disponibles las siguientes opciones:

    a. Seleccione una dirección de correo electrónico o marque su casilla de verificación correspondiente y elija View report (Ver informe) para ver los detalles. (Si se trata de una dirección que se ha agregado en forma automática a su lista de supresión debido a un rebote o reclamo, se mostrará información sobre el evento de valoración que provocó que se agregue, incluidos detalles sobre el mensaje de correo electrónico que produjo el evento desencadenador).

    b. Puede personalizar la tabla de la lista de supresión al seleccionar el icono de engranaje (se mostrará un modal en el que puede personalizar el tamaño de página, el ajuste de línea y las columnas que visualizará), después de realizar las selecciones, elija Confirm (Confirmar). La tabla de la lista de supresión reflejará sus opciones de visualización.

Eliminar de forma individual direcciones de correo electrónico de la lista de supresión de nivel de cuenta de Amazon SES

Si una dirección está en la lista de supresión de su cuenta, pero sabe que dicha dirección no debería estar en la lista, puede eliminarla mediante la operación DeleteSuppressedDestination de la API v2 de SES.

> **Note**
>
> En el procedimiento siguiente se presupone que ya ha instalado la AWS CLI. Para obtener más información sobre cómo instalar y configurar la AWS CLI, consulte la Guía del usuario de la AWS Command Line Interface.

Para eliminar direcciones individuales de la lista de supresión de nivel de cuenta con la AWS CLI

- En la línea de comandos, escriba el comando siguiente.

  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
  ```

  En el ejemplo anterior, sustituya *recipient@example.com* por la dirección de correo electrónico que desea eliminar de la lista de supresión de nivel de cuenta.

Para eliminar direcciones individuales de la lista de supresión de nivel de cuenta con la consola de SES:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Suppression list (Lista de supresión).
3. Elimine las direcciones de correo electrónico individuales mediante (a) la selección de la tabla o (b) ingresar datos:

   a. Selección de la tabla: en la tabla Suppression list (Lista de supresión), seleccione la casilla correspondiente de una o varias direcciones de correo electrónico y elija Remove (Eliminar).

   b. Ingresar datos:

      i. En la tabla Suppression list (Lista de supresión), elija Remove email address (Eliminar dirección de correo electrónico).

      ii. Escriba una dirección de correo electrónico en el campo Email address (Dirección de correo electrónico); si tiene que ingresar más direcciones, elija Enter another address (Ingresar otra dirección) y repita la acción para cada una de ellas.

iii. Cuando termine de ingresar las direcciones, revise los datos para verificar que sean correctos. Si decide que alguna de las direcciones ingresadas no debería formar parte de este envío, elija el botón Remove (Eliminar).

iv. Elija Save changes (Guardar cambios) para eliminar las direcciones de correo electrónico ingresadas de su lista de supresión de nivel de cuenta.

Eliminar en bloque direcciones de correo electrónico de la lista de supresión de nivel de cuenta de Amazon SES

Puede eliminar direcciones en bloque si carga primero su lista de contactos en un objeto de Amazon S3 seguido de la operación CreateImportJob en la API v2 de SES.

> **Note**
>
> - No hay límite para el número de direcciones que puede eliminar de la lista de supresión de nivel de cuenta, pero hay un límite de eliminación en bloque de 10 000 direcciones en un objeto de Amazon S3 por llamada a la API.
> - Si su origen de datos es un bucket de S3, debe existir en la misma región a la que se está importando.

Para eliminar direcciones de correo electrónico en bloque de su lista de supresión de nivel de cuenta, realice los pasos siguientes.

- Cargue su lista de direcciones en un objeto de Amazon S3 en formato CSV o JSON.

  Ejemplo de formato CSV para eliminar direcciones:

  ```
  recipient3@example.com
  ```

  Solo se admiten archivos JSON delimitados por saltos de línea. En este formato, cada línea es un objeto JSON completo que contiene una definición de dirección individual.

  Ejemplo de formato JSON para agregar direcciones:

  ```
  {"emailAddress":"recipient3@example.com"}
  ```

En los ejemplos anteriores, reemplace *recipient3@example.com* por las direcciones de correo electrónico que desea eliminar de la lista de supresión de nivel de cuenta.

- Conceda permiso a SES para leer el objeto de Amazon S3.

  Cuando se aplica a un bucket de Amazon S3, la siguiente política otorga permiso a SES para leer dicho bucket. Para obtener más información acerca de la asociación de políticas a buckets de Amazon S3, consulte Uso de políticas de bucket y políticas de usuario en la Guía del usuario de Amazon Simple Storage Service.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSESGet",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::BUCKET-NAME/OBJECT-NAME",
            "Condition": {
                "StringEquals": {
                    "aws:Referer": "AWSACCOUNTID"
                }
            }
        }
    ]
}
```

- Otorgue permiso a SES para utilizar su clave de AWS KMS.

  Si el objeto de Amazon S3 está cifrado con una clave de AWS KMS, debe conceder permiso a Amazon SES para que use la clave de AWS KMS. SES solo puede obtener el permiso de una clave administrada por el cliente, no de una clave de KMS predeterminada. Debe otorgar permiso a SES para utilizar la clave administrada por el cliente. Para ello, agregue una instrucción a la política de la clave.

  Pegue la siguiente instrucción de política en la política de claves para permitir que SES utilice su clave administrada por el cliente.

```
{
   "Sid": "AllowSESToDecrypt",
   "Effect": "Allow",
   "Principal": {
       "Service":"ses.amazonaws.com"
   },
   "Action": [
       "kms:Decrypt",
   ],
   "Resource": "*"
}
```

- Utilice la operación CreateImportJob en la API v2 de SES.

> **Note**
>
> En el ejemplo siguiente se presupone que ya ha instalado AWS CLI. Para obtener más información sobre cómo instalar y configurar la AWS CLI, consulte la Guía del usuario de la AWS Command Line Interface.

En la línea de comandos, escriba el comando siguiente: Reemplace *s3bucket* por el nombre del bucket de Amazon S3 y *s3object* por el nombre del objeto de Amazon S3.

```
aws sesv2 create-import-job --import-destination
 SuppressionListDestination={SuppressionListImportAction=DELETE} --import-data-source
 S3Url="s3://s3bucket/s3object",DataFormat=CSV
```

Para eliminar direcciones en bloque de la lista de supresión de nivel de cuenta mediante la consola de SES:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Suppression list (Lista de supresión).
3. En la tabla Suppression list (Lista de supresión), expanda el botón Bulk actions (Acciones masivas) y seleccione Remove email addresses in bulk (Eliminar direcciones de correo electrónico de forma masiva).

4. En Bulk action specifications (Especificaciones de acción en bloque), seleccione entre: (a) Choose file from S3 bucket (Elegir un archivo del bucket de S3) o b) Import from file (Importar desde archivo); se establecen procedimientos para cada método de importación:

   a. Choose file from S3 bucket (Elegir un archivo del bucket de S3); si el archivo de origen ya se ha almacenado en un bucket de Amazon S3:

      i. Si conoce el URI del bucket de Amazon S3 que desea utilizar, ingréselo en el campo Amazon S3 URI (URI de Amazon S3); de lo contrario, elija Browse S3 (Examinar S3):

         A. En Buckets (Buckets), elija el nombre del bucket de S3.

         B. En Objects (Objetos), seleccione el nombre del archivo y, a continuación, seleccione Choose (Elegir), esto lo redirigirá a Bulk action specifications (Especificaciones de acción masiva).

         C. (Opcional) Si desea dirigirse a la consola de Amazon S3 para ver detalles sobre su objeto de S3, elija View (Vista).

      ii. En File format (Formato de archivo), seleccione el formato del archivo que ha elegido importar desde su bucket de Amazon S3.

      iii. Elija Remove email addresses (Eliminar direcciones de correo electrónico) para iniciar la importación de direcciones de su archivo; aparecerá una tabla debajo de la pestaña Bulk actions (Acciones masivas).

   b. Import from file (Importar desde archivo), si tiene un archivo de origen local para cargar en un bucket de Amazon S3 nuevo o existente:

      i. En Import source file (Importar archivo de origen), seleccione Choose file (Elegir archivo).

      ii. Seleccione el archivo JSON o CSV en el explorador de archivos y elija Open (Abrir), verá el nombre, el tamaño y la fecha de su archivo debajo del botón Choose file (Elegir archivo).

      iii. Expanda Amazon S3 bucket (Bucket de Amazon S3) y seleccione el bucket de S3.

         - Para cargar el archivo en un bucket nuevo, elija Create S3 bucket (Crear bucket de S3), escriba un nombre en el campo Bucket name (Nombre del bucket) y elija Create bucket (Crear bucket).

      iv. Elija Remove email addresses (Eliminar direcciones de correo electrónico) para iniciar la importación de direcciones de su archivo; aparecerá una tabla debajo de la pestaña Bulk actions (Acciones masivas).

5. Independientemente del método de importación que haya utilizado, su ID de trabajo aparecerá en Bucket name (Acciones masivas), junto con el tipo de importación, el estado y la fecha; para ver los detalles del trabajo, seleccione el ID del trabajo.
6. Seleccione la pestaña Supression list (Lista de supresión) y dejarán de mostrarse todas las direcciones de correo electrónico importadas correctamente que se han eliminado de la lista de supresión.

Visualización de una lista de trabajos de importación de la cuenta

Puede ver una lista de todas las direcciones de correo electrónico que están en la lista de supresión de nivel de cuenta de la cuenta mediante la operación ListImportJobs en la API v2 de Amazon SES.

> **Note**
>
> En el procedimiento siguiente se presupone que ya ha instalado la AWS CLI. Para obtener más información sobre cómo instalar y configurar la AWS CLI, consulte la Guía del usuario de la AWS Command Line Interface.

Para ver una lista de todos los trabajos de importación de la cuenta

- En la línea de comandos, escriba el comando siguiente.

```
aws sesv2 list-import-jobs
```

El comando anterior devuelve todos los trabajos de importación de la cuenta. La salida se parece al siguiente ejemplo:

```
{
    "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"
        }
    ]
}
```

Para ver una lista de todos los trabajos de importación de la cuenta mediante la consola de SES:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Suppression list (Lista de supresión).
3. En el panel Supresión list (Lista de supresión), seleccione la pestaña Bulk actions (Acciones masivas).
4. Todos los trabajos de importación aparecerán en la tabla Bulk actions (Acciones masivas) junto con el tipo, el estado y la fecha de importación.
5. Para ver los detalles del trabajo, seleccione el ID de trabajo y aparecerán los siguientes paneles:

    a. Bulk action status (Estado de acción masiva): muestra el estado general de los trabajos, la hora y la fecha en que se completaron, cuántos registros se importaron y el recuento de los registros que no se han podido importar correctamente.

b. Bulk action details (Detalles de acción masiva): muestra el ID de trabajo, si se utilizó para agregar o eliminar direcciones, si el formato de archivo era JSON o CSV, el URI del bucket de Amazon S3 donde se almacenó el archivo masivo y la fecha y hora de creación de la acción masiva.

Obtención de información acerca de un trabajo de importación de la cuenta

Puede obtener información acerca de un trabajo de importación de la cuenta mediante la operación GetImportJob en la API v2 de Amazon SES.

> **Note**
>
> En el procedimiento siguiente se presupone que ya ha instalado la AWS CLI. Para obtener más información sobre cómo instalar y configurar la AWS CLI, consulte la Guía del usuario de la AWS Command Line Interface.

Para obtener información acerca de un trabajo de importación de la cuenta

- En la línea de comandos, escriba el comando siguiente.

```
aws sesv2 get-import-job --job-id JobId
```

El comando anterior devuelve información acerca de un trabajo de importación de la cuenta. La salida se parece al siguiente ejemplo:

```
{
    "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"
}
```

Para obtener información sobre un trabajo de importación de la cuenta mediante la consola de SES:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Suppression list (Lista de supresión).
3. En el panel Supresión list (Lista de supresión), seleccione la pestaña Bulk actions (Acciones masivas).
4. Todos los trabajos de importación aparecerán en la tabla Bulk actions (Acciones masivas) junto con el tipo, el estado y la fecha de importación.
5. Para ver los detalles del trabajo, seleccione el ID de trabajo y aparecerán los siguientes paneles:

    a. Bulk action status (Estado de acción masiva): muestra el estado general de los trabajos, la hora y la fecha en que se completaron, cuántos registros se importaron y el recuento de los registros que no se han podido importar correctamente.

    b. Bulk action details (Detalles de acción masiva): muestra el ID de trabajo, si se utilizó para agregar o eliminar direcciones, si el formato de archivo era JSON o CSV, el URI del bucket de Amazon S3 donde se almacenó el archivo masivo y la fecha y hora de creación de la acción masiva.

Desactivar la lista de supresión de nivel de cuenta de Amazon SES

Puede utilizar la operación PutAccountSuppressionAttributes de la API v2 de SES para desactivar la lista de supresión de nivel de cuenta de forma eficaz mediante la eliminación de los valores del atributo `suppressed-reasons`.

> **Note**
>
> En el procedimiento siguiente se presupone que ya ha instalado la AWS CLI. Para obtener más información sobre cómo instalar y configurar la AWS CLI, consulte la Guía del usuario de la AWS Command Line Interface.

Para desactivar la lista de supresión de nivel de cuenta mediante la AWS CLI

- En la línea de comandos, escriba el comando siguiente.

```
aws sesv2 put-account-suppression-attributes --suppressed-reasons
```

Para desactivar la lista de supresión de nivel de cuenta mediante la consola de SES:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Suppression list (Lista de supresión).
3. En el panel Account-level settings (Configuración de nivel de cuenta), seleccione Edit (Editar).
4. En Suppression list (Lista de supresión), desmarque la casilla Enabled (Habilitado).
5. Elija Guardar cambios.

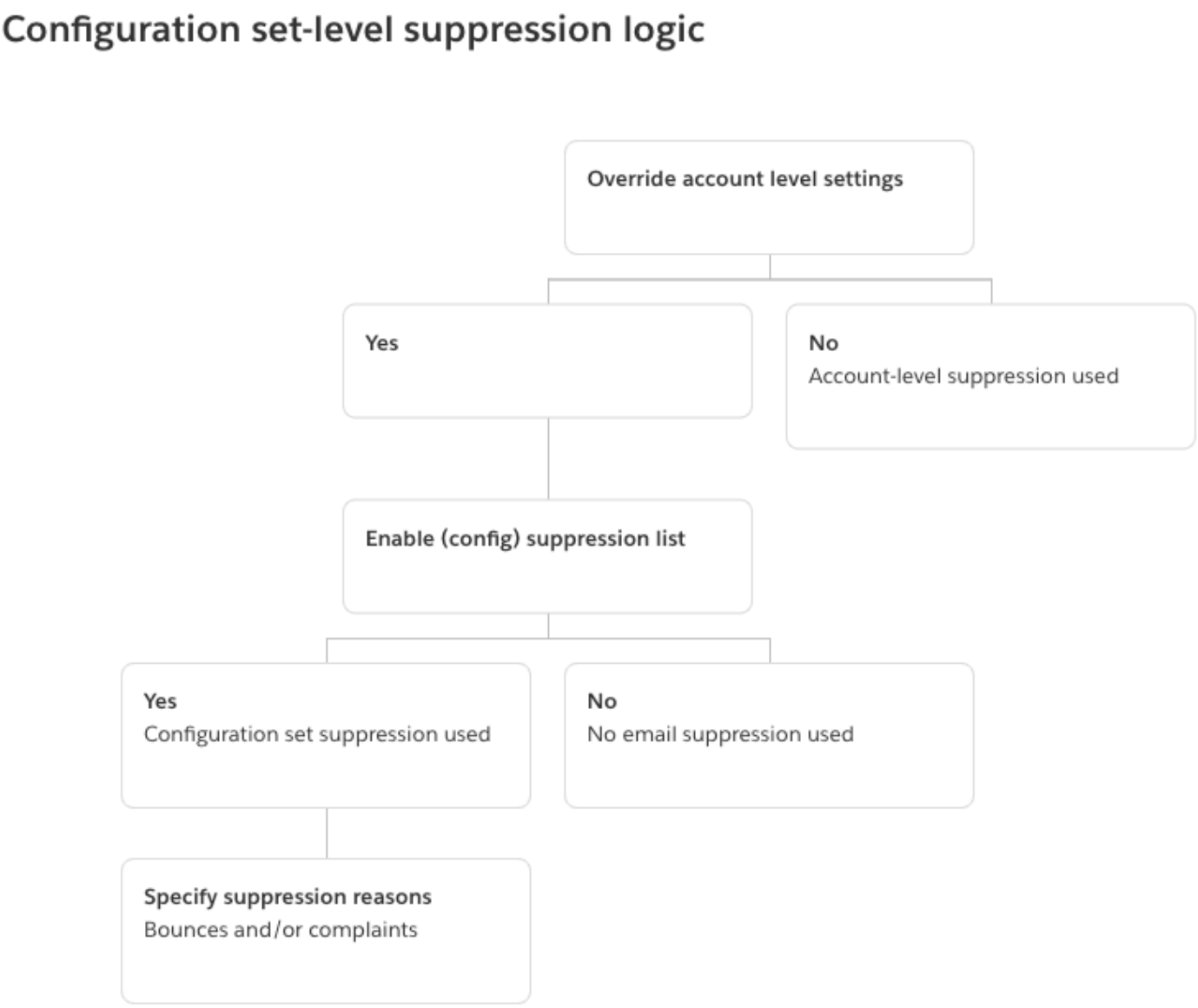
Uso de la supresión de nivel de conjunto de configuración para invalidar la lista de supresión de nivel de cuenta

Aunque la lista de supresión de nivel de cuenta está configurada para toda la cuenta, puede personalizarla de forma individual para distintos conjuntos de configuración invalidándola con la supresión de nivel de conjunto de configuración. Este nivel más detallado le permite utilizar configuraciones de supresión personalizadas para diferentes grupos de envío de correo electrónico que ha asignado a sus propios conjuntos de configuración. Por ejemplo, supongamos que la lista de supresión de nivel de cuenta está configurada para agregar direcciones de rebote y reclamación, pero tiene un determinado grupo demográfico de correo electrónico definido en un conjunto de configuración para el que solo le interesa agregar direcciones de reclamaciones; lo lograría habilitando estas invalidaciones de supresión del conjunto de configuración para que las direcciones

de correo electrónico se agreguen a la lista de supresión de nivel de cuenta solo para reclamaciones (no rebotes y reclamaciones como se establece en la lista de supresión de nivel de cuenta) desde el correo electrónico enviado con este conjunto de configuración.

Con la supresión de nivel de conjunto de configuración, existen diferentes niveles de invalidación de la supresión de nivel de cuenta, incluso no utilizar ninguna supresión. Para ayudar a comprender estos distintos niveles de supresión que se pueden establecer en los siguientes procedimientos de la consola, el siguiente mapa de relaciones ilustra el conjunto de decisiones que puede tomar para habilitar o desactivar varios niveles de invalidaciones, que, según su combinación, se pueden utilizar para implementar tres niveles diferentes de supresión:

- Sin invalidaciones (predeterminado): el conjunto de configuración utiliza los ajustes de la lista de supresión de nivel de cuenta.
- Invalidar la configuración de nivel de cuenta: esto anulará cualquier configuración de lista de supresión de nivel de cuenta; el correo electrónico enviado con este conjunto de configuración no utilizará ninguna configuración de supresión.
- Invalidar la configuración de nivel de cuenta con la supresión de nivel de conjunto de configuración habilitada: el correo electrónico enviado con este conjunto de configuración solo utilizará las condiciones de supresión habilitadas para él (rebotes, reclamaciones o rebotes y reclamaciones). Independientemente de la configuración de la lista de supresión de nivel de cuenta, la invalidará.



Tenga en cuenta que la supresión de nivel de conjunto de configuración no es una lista de supresión real, es su lugar, es simplemente un mecanismo para invalidar la lista de supresión de nivel de cuenta con configuraciones de supresión personalizadas definidas en un conjunto de configuración; esto significa que cualquier correo electrónico enviado con el conjunto de configuración solo utilizará su propia configuración de supresión e ignorará cualquier configuración de supresión de nivel de cuenta. En otras palabras, la supresión de nivel de conjunto de configuración interactúa con la lista de supresión a nivel de cuenta simplemente cambiando (invalidando) los motivos de supresión que determinan qué direcciones de correo electrónico se agregan a la lista de supresión de nivel de cuenta.

Habilitar la supresión de nivel de conjunto de configuración

Para habilitar la supresión de nivel de conjunto de configuración mediante la nueva consola de Amazon SES:

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, en Configuration (Configuración), elija Configuration sets (Conjuntos de configuración).
3. En Configuration sets (Conjuntos de configuración), elija el nombre del conjunto de configuración que desea configurar con supresión personalizada.
4. En el panel Suppression list options (Opciones de lista de supresión), elija Edit (Editar).
5. La sección Suppression list options (Opciones de lista de supresión) proporciona un conjunto de decisiones para definir la supresión personalizada, a partir de la opción de utilizar este conjunto de configuración para anular la supresión de nivel de cuenta. El mapa lógico de supresión de nivel de conjunto de configuración le ayudará a comprender los efectos de las combinaciones de anulación. Estas selecciones de anulaciones de varios niveles se pueden combinar para implementar tres niveles diferentes de supresión:

   a. Use account-level suppression (Utilizar supresión de nivel de cuenta): no anular la supresión de nivel de cuenta y no implementar ninguna supresión de nivel de conjunto de configuración; básicamente, cualquier correo electrónico enviado con este conjunto de configuración solo utilizará la supresión de nivel de cuenta. Para ello:

      - En Suppression list settings (Configuración de lista de supresión), desmarque la casilla Override account level settings (Anular la configuración de nivel de cuenta).

   b. Do not use any suppression (No utilizar ninguna supresión): anular la supresión de nivel de cuenta sin habilitar ninguna supresión de nivel de conjunto de configuración; esto significa que cualquier correo electrónico enviado con este conjunto de configuración no utilizará ninguna supresión de nivel de cuenta; en otras palabras, se cancelará toda supresión. Para ello:

      i. En Suppression list settings (Configuración de lista de supresión), marque la casilla Override account level settings (Anular la configuración de nivel de cuenta).

      ii. En Suppression list (Lista de supresión), desmarque la casilla Enabled (Habilitado).

c. Use configuration set-level suppression (Utilizar supresión de nivel de conjunto de configuración): invalide la lista de supresión de nivel de cuenta con configuraciones de supresión personalizadas definidas en este conjunto de configuración; esto significa que cualquier correo electrónico enviado con este conjunto de configuración solo utilizará su propia configuración de supresión e ignorará cualquier configuración de supresión de nivel de cuenta. Para ello:

   i. En Suppression list settings (Configuración de lista de supresión), marque la casilla Override account level settings (Anular la configuración de nivel de cuenta).

   ii. En Suppression list (Lista de supresión), marque Enabled (Habilitado).

   iii. En Specify the reason(s)... [Especificar el motivo (s)...], seleccione uno de los motivos de supresión que utilizará este conjunto de configuración.

6. Elija Save changes.

Uso de la administración de listas

Amazon SES ofrece funciones de administración de listas, lo que significa que los clientes pueden administrar sus propias listas de correo, conocidas como listas de contactos. Una lista de contactos es una lista que le permite almacenar todos sus contactos que se han suscrito a uno o varios temas concretos. Un contacto es un usuario final que recibe sus mensajes de correo electrónico. Un tema es un grupo de interés, un tema o una etiqueta de una lista. Las listas pueden tener varios temas.

Al usar la operación `ListContacts` de la API v2 de Amazon SES, puede recuperar una lista de todos los contactos que se han suscrito a un tema concreto, a los que puede enviar mensajes de correo electrónico mediante la operación `SendEmail`.

Para obtener más información acerca de la administración de suscripciones, consulte Uso de la administración de suscripciones.

Información general acerca de la administración de listas

Debe tener en cuenta los siguientes factores cuando utilice la administración de listas:

- Puede especificar temas de lista al crear la lista.
- Solo se permite una lista de contactos por Cuenta de AWS.
- Una lista puede tener un máximo de 20 temas.

- Puede actualizar una lista de contactos existente, lo que incluye agregar nuevos temas a la lista, agregar o eliminar contactos de una lista y actualizar las preferencias de contacto de una lista o un tema.
- Puede actualizar los metadatos del tema, como el nombre para mostrar o la descripción del tema.
- Puede obtener una lista de contactos de una lista de contactos, contactos suscritos a un tema, contactos cuya suscripción a un tema se ha cancelado y contactos cuya suscripción a todos los temas de la lista se ha cancelado.
- Puede importar las listas de contactos existentes en Amazon SES mediante la API `CreateImportJob`.
- Amazon SES rebotará un correo electrónico si se envía a un contacto cuya suscripción se ha cancelado en su lista de contactos. Para obtener más información, consulte Uso de la administración de suscripciones.
- Cada contacto puede tener atributos asociados que puede utilizar para almacenar información acerca de ese contacto.

Configuración de la administración de listas

Puede utilizar las siguientes operaciones para configurar las capacidades de administración de listas. Para obtener la lista completa de la lista de contactos y las operaciones de contactos, consulte la Referencia de la API v2 de Amazon SES.

Creación de una lista de contactos

Puede utilizar la operación `CreateContactList` en la API v2 de Amazon SES para crear una lista de contactos. Para establecer esta configuración de forma rápida y fácil, utilice la AWS CLI. Para obtener más información sobre cómo instalar y configurar la AWS CLI, consulte la Guía del usuario de la AWS Command Line Interface.

Para crear un conjunto de configuración mediante AWS CLI

- En la línea de comandos, escriba el comando siguiente.

  ```
  aws sesv2 create-contact-list --cli-input-json file://CONTACT-LIST-JSON
  ```

  En el comando anterior, reemplace *CONTACT-LIST-JSON* por la ruta del archivo JSON para su solicitud `CreateContactList`.

Un archivo JSON de entrada `CreateContactList` de ejemplo para la solicitud es como el siguiente:

```
{
    "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"
     }
    ]
}
```

Creación de un contacto

Puede utilizar la operación `CreateContact` en la API v2 de Amazon SES para crear un contacto. Para establecer esta configuración de forma rápida y fácil, utilice la AWS CLI. Para obtener más información sobre cómo instalar y configurar la AWS CLI, consulte la Guía del usuario de la AWS Command Line Interface.

Para crear un contacto mediante AWS CLI

- En la línea de comandos, escriba el comando siguiente.

```
aws sesv2 create-contact --cli-input-json file://CONTACT-JSON
```

En el comando anterior, reemplace *CONTACT-JSON* por la ruta del archivo JSON para la solicitud `CreateContact`.

Un archivo JSON de entrada `CreateContact` de ejemplo para la solicitud es como el siguiente:

```
{
    "ContactListName": "ExampleContactListName",
    "EmailAddress": "example@amazon.com",
    "UnsubscribeAll": false,
    "TopicPreferences": [
        {
            "TopicName": "Sports",
            "SubscriptionStatus": "OPT_IN"
        }
    ],
    "AttributesData": "{\"Name\": \"John\", \"Location\": \"Seattle\"}"
}
```

En el ejemplo anterior, un valor `UnsubscribeAll` de `false` muestra que el contacto no ha cancelado la suscripción de todos los temas, donde un valor de `true` significaría que se ha cancelado la suscripción del contacto de todos los temas.

`TopicPreferences` incluye información acerca del estado de suscripción del contacto a los temas. En el ejemplo anterior, el contacto ha optado por el tema "Sports" (Deportes) y recibirá todos los mensajes de correo electrónico para el tema "Sports" (Deportes).

`AttributesData` es un campo JSON donde puede poner los metadatos acerca de nuestro contacto. Debe ser un objeto JSON válido.

Importación en bloque de contactos a su lista de contactos

Puede agregar direcciones manualmente en bloque si carga primero los contactos en un objeto de Simple Storage Service (Amazon S3) seguido de la operación `CreateImportJob` en la API v2 de Amazon SES o mediante la consola de SES. Para obtener más información, consulte Agregar direcciones de correo electrónico en bloque a la lista de supresión de nivel de cuenta.

Debe crear una lista de contactos antes de importar los contactos.

> **Note**
>
> Puede agregar hasta 1 millón de contactos a una lista de contactos por operación ImportJob.

Para agregar contactos en bloque a su lista de contactos, realice los pasos siguientes.

- Cargue sus contactos en un objeto de Amazon S3 en formato CSV o JSON.

  CSV format (Formato CSV)

  La primera línea del archivo que se carga en Amazon S3 debe ser una línea de encabezado.

  El objeto `topicPreferences` se debe aplanar para el formato CSV. Cada tema en `topicPreferences` tendrá un campo de encabezado independiente.

  Ejemplo de formato CSV para agregar contactos en bloque a una lista de contactos:

```
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
```

  Formato JSON

Solo se admiten archivos JSON delimitados por saltos de línea. En este formato, cada línea es un objeto JSON completo que contiene la información de un contacto.

Ejemplo de formato JSON para agregar contactos en bloque a una lista de contactos:

```
{
     "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"
      }
     ]
}
```

En los ejemplos anteriores, reemplace *example1@amazon.com* y *example2@amazon.com* con las direcciones de correo electrónico que desea agregar a la lista de contactos. Reemplace los valores de `attributesData` por los valores específicos del contacto. Además, reemplace

Sports (Deportes) y *Cycling* (Ciclismo) por `topicName` que se aplica al contacto. Los `topicPreferences` aceptables son *OPT_IN* y *OPT_OUT*.

Los siguientes atributos se admiten al cargar sus contactos en un objeto de Amazon S3 en formato CSV o JSON:

Atributo	Descripción
`emailAddress`	La dirección de correo electrónico del contacto. Este es un campo obligatorio.
`unsubscribeAll`	Estado de valor booleano que indica si se ha cancelado la suscripción del contacto de todos los temas de la lista de contactos.
`topicPreferences`	Preferencias del contacto para su inclusión o exclusión en los temas.
`attributesData`	Datos de atributo asociados a un contacto.

- Conceda permiso a Amazon SES para leer el objeto de Amazon S3.

  Cuando se aplica a un bucket de Amazon S3, la siguiente política otorga permiso a Amazon SES para leer dicho bucket. Para obtener más información acerca de la asociación de políticas a buckets de Amazon S3, consulte Uso de políticas de bucket y políticas de usuario en la Guía del usuario de Amazon Simple Storage Service.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSESGet",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::BUCKET-NAME/OBJECT-NAME",
            "Condition": {
                "StringEquals": {
                    "aws:Referer": "AWSACCOUNTID"
```

```
                }
            }
        }
    ]
}
```

- Otorgue permiso a Amazon SES para utilizar su clave de AWS KMS.

  Si el objeto de Amazon S3 está cifrado con una clave de AWS KMS, debe conceder permiso a Amazon SES para que utilice la clave de KMS. Amazon SES solo puede obtener el permiso de una clave administrada por el cliente, no de una clave de KMS predeterminada. Debe otorgar permiso a Amazon SES para utilizar la clave administrada por el cliente. Para ello, agregue una instrucción a la política de la clave.

  Pegue la siguiente instrucción de política en la política de claves para permitir que Amazon SES utilice su clave administrada por el cliente.

```
{
   "Sid": "AllowSESToDecrypt",
   "Effect": "Allow",
   "Principal": {
       "Service":"ses.amazonaws.com"
   },
   "Action": [
       "kms:Decrypt",
   ],
   "Resource": "*"
}
```

- Utilice la operación `CreateImportJob` en la API v2 de Amazon SES.

> **Note**
>
> En el ejemplo siguiente se presupone que ya ha instalado AWS CLI. Para obtener más información sobre cómo instalar y configurar la AWS CLI, consulte la Guía del usuario de la AWS Command Line Interface.

En la línea de comandos, escriba el comando siguiente: Reemplace *s3bucket* por el nombre del bucket de Amazon S3 y *s3object* por el nombre del objeto de Amazon S3.

```
aws sesv2 create-import-job --import-destination
 ContactListDestination={ContactListName=ExampleContactListName,ContactListImportAction=PUT}
 --import-data-source S3Url="s3://s3bucket/s3object",DataFormat=CSV
```

Tutorial de administración de listas con ejemplos

El siguiente tutorial proporciona ejemplos de cómo puede utilizar la administración de listas para mostrar los contactos, utilizar `ListManagementOptions` para especificar una lista de contactos y un nombre de tema en el correo electrónico y cómo insertar enlaces de cancelación de suscripción.

1. Mostrar contactos mediante AWS CLI: puede usar la operación `ListContacts` para recuperar una lista de todos los contactos que se han suscrito a un tema particular, junto con la operación `SendEmail`, que le permite enviarles mensajes de correo electrónico.

   En la línea de comandos, escriba el comando siguiente.

   ```
   aws sesv2 list-contacts --cli-input-json file://LIST-CONTACTS-JSON
   ```

   En el comando anterior, reemplace *`LIST-CONTACTS-JSON`* por la ruta del archivo JSON para la solicitud de `ListContacts`.

   Un archivo JSON de entrada `ListContacts` de ejemplo para la solicitud es como el siguiente:

   ```
   {
       "ContactListName": "ExampleContactListName",
       "Filter": {
           "FilteredStatus": "OPT_IN",
           "TopicFilter": {
               "TopicName": "Cycling",
               "UseDefaultIfPreferenceUnavailable": true
           }
       },
       "PageSize": 50
   }
   ```

   `FilteredStatus` muestra el estado de suscripción por el que desea filtrar, que es `OPT_IN` o `OPT_OUT`.

   `TopicFilter` es un filtro opcional que especifica el tema del que desea obtener resultados, que en el ejemplo anterior es "Cycling" (Ciclismo).

`UseDefaultIfPreferenceUnavailable` puede tener un valor de `true` o `false`. Si es `true`, se usará la preferencia de tema predeterminada si el contacto no tiene ninguna preferencia explícita para un tema. Si es `false`, solo se tienen en cuenta los contactos con una preferencia establecida explícita para el filtrado.

2. Enviar correo con **`ListManagementOptions`** habilitado: después de mostrar los contactos en la lista utilizando la operación `ListContacts` anterior, puede utilizar la operación `SendEmail` para enviar correos electrónicos a cada uno de los contactos mediante el encabezado `ListManagementOptions` para especificar la lista de contactos y el nombre del tema.

   Para utilizar `ListManagementOptions` con la operación `SendEmail`, incluya `contactListName` y `topicName` al que pertenece el correo electrónico (`topicName` es opcional):

   ```
   ListManagementOptions:
       String contactListName
       String topicName
   ```

   Si incluye `ListManagementOptions` en la solicitud `SendEmail` a una dirección de correo electrónico de destinatario que no está en la lista de contactos, se creará un contacto en la lista automáticamente.

   Amazon SES rebotará un mensaje de correo electrónico si se envía a un contacto cuya suscripción se ha cancelado en la lista de contactos, lo que significa que no tendrá que actualizar las solicitudes `SendEmail` para evitar el envío a contactos cuya suscripción se ha cancelado.

3. Indicar la ubicación de los enlaces de cancelación de suscripción: al utilizar `ListManagementOptions` tiene la opción de permitir que Amazon SES agregue enlaces de pie de página de cancelación de suscripción en el correo electrónico mediante el marcador de posición `{{amazonSESUnsubscribeUrl}}` para especificar dónde debe insertar SES la URL de cancelación de suscripción. Solo se admite el reemplazo de marcadores de posición para los tipos de contenido HTML y TEXT. Puede incluir el marcador de posición dos veces como máximo. Si se utiliza más de dos veces, solo se reemplazan las dos primeras coincidencias. Para obtener más información, consulte Uso de la administración de suscripciones.

Otra opción, si utiliza la interfaz de SMTP para enviar un correo electrónico, puede usar el encabezado `X-SES-LIST-MANAGEMENT-OPTIONS` para especificar una lista y un nombre de tema.

Para especificar una lista y un nombre de tema durante el envío de correo electrónico mediante la interfaz SMTP, agregue el siguiente encabezado de correo electrónico al mensaje:

```
X-SES-LIST-MANAGEMENT-OPTIONS: {contactListName}; topic={topicName}
```

Uso de la administración de suscripciones

Amazon SES proporciona una capacidad de administración de suscripciones, en la que Amazon SES habilita automáticamente los enlaces de cancelación de suscripción en cada correo electrónico saliente cuando especifica `contactListName` y `topicName` dentro de `ListManagementOptions` en la solicitud de la operación `SendEmail`.

Si un contacto cancela la suscripción a un tema o una lista en particular, Amazon SES no permite el envío de correo electrónico al contacto para ese tema o esa lista en el futuro.

> **Note**
>
> - La gestión de suscripciones de Amazon SES cumple con los requisitos de envío masivo exigidos por muchos proveedores de servicios de correo electrónico; consulte la sección 2 en Descripción general de los cambios en los envíos masivos para obtener más información.
> - La administración de suscripciones está disponible para aquellos que utilizan Easy DKIM en Amazon SES, pero Amazon SES no puede agregar los vínculos de cancelación de suscripción a su correo electrónico para los remitentes que firman los mensajes de correo electrónico antes de llamar a Amazon SES.

Para obtener información sobre la administración de listas y sobre cómo utilizarla, incluida la recuperación de una lista de todos los contactos que se han suscrito a un tema concreto, consulte Uso de la administración de listas.

Información general acerca de la administración de suscripciones

Debe tener en cuenta los siguientes factores cuando utilice la administración de suscripciones:

- Amazon SES administrará por completo las suscripciones. Esto significa que Amazon SES recibe correos electrónicos y solicitudes de cancelación de suscripción de la página web de cancelación de suscripción y, a continuación, actualiza las preferencias del contacto en su lista. Puede recibir notificaciones de cancelación de suscripción mediante notificaciones de conjunto de configuración. Para obtener más información acerca de los conjuntos de configuración, consulte Uso de conjuntos de configuración en Amazon SES.
- Debe especificar la lista de contactos mientras envía el correo electrónico. La administración de suscripciones a través de los enlaces del encabezado `List-Unsubscribe` y el pie de página `ListManagementOptions` se gestionarán en consecuencia.
- Amazon SES agrega compatibilidad con los estándares de encabezado `List-Unsubscribe`, que permitirán a los clientes de correo electrónico y a los proveedores de la bandeja de entrada mostrar un enlace de cancelación de suscripción en la parte superior del correo electrónico si lo admiten, no todos los proveedores de servicio de correo electrónico admiten estos encabezados.
- Los encabezados `List-Unsubscribe` siguen el comportamiento que se muestra a continuación:
  - Si un contacto hace clic en el enlace de cancelar suscripción en un correo electrónico que tiene la lista de contactos y el tema especificados, solo se cancelará la suscripción del contacto de ese tema específico.
  - Si no se especifica el tema, se cancelará la suscripción del contacto de todos los temas de la lista.
- Los contactos se llevarán a una página de destino para cancelar la suscripción cuando hagan clic en el enlace correspondiente en el pie de página del correo electrónico.
- La página de destino para cancelar la suscripción proporcionará a los contactos una opción para actualizar sus preferencias, lo que significa `OPT_IN` o `OPT_OUT`, para todos los temas de una lista en particular. La página de destino también ofrece la opción de cancelar la suscripción de todos los temas de la lista.
- Si utiliza `ListManagementOptions`, debe incluir un marcador de posición `{{amazonSESUnsubscribeUrl}}` en los correos electrónicos para indicar dónde debe insertar Amazon SES la URL de cancelación de suscripción. Puede incluir el marcador de posición dos veces como máximo. Si se utiliza más de dos veces, solo se reemplazan las dos primeras coincidencias.

- Los enlaces del encabezado `List-Unsubscribe` y el pie de página `ListManagementOptions` se agregan solo si el correo electrónico se envía a un único destinatario.
- Para los correos electrónicos de transacciones en los que no desea que los contactos puedan cancelar la suscripción, puede omitir el campo `ListManagementOptions` con la solicitud de `SendEmail`.

Consideraciones sobre el encabezado de cancelación de suscripción

La administración de suscripciones mediante un enlace de cancelación de suscripción está habilitada cuando el correo electrónico contiene los siguientes encabezados:

`List-Unsubscribe`

`List-Unsubscribe-Post`

Cuando utiliza la administración de suscripciones de Amazon SES, `ListManagementOptions`, Amazon SES invalidará estos encabezados si están presentes en el correo electrónico.

Los destinatarios que cancelen la suscripción haciendo clic en el enlace producido por estos encabezados tendrán una experiencia diferente según el cliente de correo electrónico o el proveedor de la bandeja de entrada porque algunos proveedores no reconocen los encabezados `List-Unsubscribe` y `List-Unsubscribe-Post`; el correo electrónico enviado a los destinatarios utilizando dichos proveedores no verá el enlace Cancelar suscripción.

Los destinatarios cuyo cliente de correo electrónico reconozca estos encabezados verán el enlace Cancelar suscripción y podrán cancelar la suscripción a través del enlace pero no tendrán la opción de elegir los temas de los que quieren cancelar la suscripción. Simplemente se cancelará la del tema para el que se envió el correo electrónico.

Para obtener más información sobre el encabezado `List-Unsubscribe`, consulte RFC 2369 y para el encabezado `List-Unsubscribe-Post`, consulte RFC 8058.

> **Note**
>
> Amazon SES admite la cancelación de la suscripción con un clic de acuerdo con los requisitos de envío masivo exigidos por muchos proveedores de servicios de correo electrónico. Para obtener más información, consulte Uso de la cancelación de suscripción con un clic con Amazon SES.

Agregar un vínculo de pie de página de cancelación de suscripción

Tendrá que utilizar el marcador de posición `{{amazonSESUnsubscribeUrl}}` en correos electrónicos con plantilla y sin plantilla para especificar dónde debe insertar Amazon SES la URL de cancelación de suscripción.

Solo se admite el reemplazo de marcadores de posición para los tipos de contenido HTML y TEXT.

Puede incluir el marcador de posición dos veces como máximo. Si se utiliza más de dos veces, solo se reemplazan las dos primeras coincidencias.

> **Note**
>
> El marcador de posición `{{amazonSESUnsubscribeUrl}}` solo se puede utilizar si se especifica `ListManagementOptions` como encabezado mientras se utiliza la operación `SendEmail` o X-SES-LIST-MANAGEMENT-OPTIONS se especifica como un encabezado al utilizar la interfaz de SMTP. (No se debe confundir con los encabezados `List-Unsubscribe` o `List-Unsubscribe-Post` que no dependen de `ListManagementOptions` y se pueden utilizar por sí mismos.)

Monitoreo de la actividad de envío de Amazon SES

Amazon SES ofrece métodos para monitorear la actividad de envío mediante eventos, métricas y estadísticas. Un evento es algo que ocurre en relación con la actividad de envío que ha especificado para que se rastree como métrica. Un métrica representa una serie de puntos de datos ordenados por tiempo que representa los valores de un tipo de evento monitoreado que produce estadísticas. Las estadísticas son agregaciones de los datos de las métricas correspondientes a un periodo de tiempo especificado, incluso hasta el presente.

Estos métodos de supervisión lo ayudan a realizar un seguimiento de medidas importantes, como, por ejemplo, las tasas de rebotes, reclamos y rechazos de su cuenta. Unas tasas de rebotes y reclamos demasiado altas podrían comprometer su capacidad de enviar correos electrónicos a través de SES. Estos métodos también se pueden utilizar para medir las tasas a las que los clientes interactúan con los correos electrónicos que envía, lo que lo ayuda a identificar las tasas generales de apertura y clics mediante la publicación de eventos y los dominios personalizados asociados con los conjuntos de configuración. Consulte Configuración de dominios personalizados para gestionar seguimiento de mensajes abiertos y en los que se ha hecho clic.

El primer paso para configurar la supervisión es identificar los tipos de eventos de correo electrónico relacionados con la actividad de envío que desea medir y monitorear mediante SES. Puede elegir los siguientes tipos de eventos para monitorear en SES:

- Send (Envío): la solicitud de envío se realizó de forma correcta y Amazon SES intentará entregar el mensaje al servidor de correo del destinatario. (Si se está utilizando la supresión global o de nivel de cuenta, SES lo seguirá contando como un envío, pero la entrega se suprimirá).
- RenderingFailure— El correo electrónico no se envió debido a un problema de representación de la plantilla. Este tipo de evento se puede producir cuando faltan datos en la plantilla o cuando los parámetros y los datos de la plantilla no coinciden. (Este tipo de evento solo se produce cuando envía correo electrónico con las operaciones de la API `SendTemplatedEmail` o `SendBulkTemplatedEmail`).
- Reject (Rechazo): Amazon SES aceptó el correo electrónico, pero determinó que contenía un virus y no intentó entregarlo al servidor de correo del destinatario.
- Delivery (Entregados): Amazon SES entregó correctamente el correo electrónico al servidor de correo del destinatario.

- Rebotar: una devolución permanente que el servidor de correo del destinatario ha rechazado el correo electrónico de forma permanente. (Los rebotes temporales solo se incluyen cuando Amazon SES no puede entregar el correo electrónico tras intentarlo durante un periodo de tiempo).
- Complaint (Reclamo): el correo electrónico se entregó correctamente al servidor de correo del destinatario, pero el destinatario lo marcó como spam.
- DeliveryDelay— No se pudo entregar el correo electrónico al servidor de correo del destinatario porque se produjo un problema temporal. Pueden producirse retrasos en la entrega, por ejemplo, si la bandeja de entrada del destinatario está llena o el servidor de recepción de email experimenta un problema transitorio.
- Subscriptions (Suscripciones): el correo electrónico se entregó correctamente, pero el destinatario actualizó las preferencias de suscripción al hacer clic en `List-Unsubscribe` en el encabezado del correo electrónico o el enlace `Unsubscribe` del pie de página.
- Open (Abiertos): el destinatario recibió el mensaje y lo abrió en su cliente de correos electrónicos.
- Clic: el destinatario hizo clic en uno o varios enlaces incluidos en el correo electrónico.

Puede monitorear los eventos de envío de correo electrónico de varias maneras. El método que elija dependerá del tipo de evento que desee monitorear, la granularidad y el nivel de detalle con los que quiera monitorearlos, así como de la ubicación en la que desea que Amazon SES publique los datos. Debe utilizar las notificaciones de retroalimentación o la publicación de eventos para realizar un seguimiento de los eventos de rebotes y reclamaciones. También puede optar por utilizar varios métodos de monitorización. Las características de cada método se indican en la siguiente tabla.

Método de monitorización	Eventos que puede monitorizar	Cómo acceder a los datos	Nivel de detalle	Granularity (Grado de detalle)
Consola de Amazon SES	Estado de la cuenta, correos electrónicos enviados, cuota utilizada, solicitudes de envío satisfactorias, rechazos, rebotes y	Página del panel de la cuenta en la consola de Amazon SES	Recuento y porcentaje	En toda la cuenta de AWS

Método de monitorización	Eventos que puede monitorizar	Cómo acceder a los datos	Nivel de detalle	Granularity (Grado de detalle)
	reclamos (historial reciente de la reputación actual)			
Consola de Amazon SES	Estado de la cuenta, correos electrónicos enviados, rebotes y reclamos (reputación actual)	Página de métricas de reputación en la consola de Amazon SES	Solo tarifas calculadas	En toda la cuenta de AWS
API de Amazon SES	Entregas, rebotes, reclamaciones y rechazos	`GetSendStatistics` Operación de la API	Recuento solo	En toda la cuenta de AWS

Método de monitorización	Eventos que puede monitorizar	Cómo acceder a los datos	Nivel de detalle	Granularity (Grado de detalle)
CloudWatch Consola Amazon	Envíos, entregas, aperturas, clics, devoluciones, tasa de devoluciones, reclamaciones, tasa de reclamaciones, rechazos, errores de representación e IP en la lista negra.	CloudWatch consola **Note** Algunas métricas no aparecen CloudWatch hasta que se produce el evento asociado. Por ejemplo, las métricas de rebote no aparecen CloudWatch hasta que se devuelve al menos un correo electrónico que envíes	Recuento solo	En toda la cuenta de AWS

Método de monitorización	Eventos que puede monitorizar	Cómo acceder a los datos	Nivel de detalle	Granularity (Grado de detalle)
		o hasta que generes un evento de rebote simulado mediante el simulador de buzones de correo.		
Notificaciones de retroalimentación	Entregas, rebotes y reclamaciones	Notificación de Amazon SNS (entregas, rebotes y reclamos) o correo electrónico (solo rebotes y reclamos). Consulte Configuración de notificaciones de eventos.	Detalles de cada evento	En toda la cuenta de AWS

Método de monitorización	Eventos que puede monitorizar	Cómo acceder a los datos	Nivel de detalle	Granularity (Grado de detalle)
Publicación de eventos	Envíos, entregas, abiertos, clics, rebotes, reclamaciones, rechazos y errores de representación.	Amazon CloudWatch o Amazon Data Firehose, o mediante una notificación de Amazon SNS (consulte . Supervisar el envío de correo electrónico mediante la publicación de eventos (Se aplican cargos adicionales; consulte el precio por métrica para ver.) CloudWatch	Detalles de cada evento	Detallado (basado en características de correo electrónico definibles por el usuario)

Método de monitorización	Eventos que puede monitorizar	Cómo acceder a los datos	Nivel de detalle	Granularity (Grado de detalle)
Publicación de eventos mediante dominios personalizados asociados a conjuntos de configuración: más información	Abra y haga clic en Tracking (Seguimiento).	Amazon CloudWatch o Amazon Data Firehose, o mediante notificación de Amazon SNS. (Se aplican cargos adicionales; consulte el precio por métrica para CloudWatch ver.)	Detalles de cada evento.	Detallado (basado en características de correo electrónico definibles por el usuario)

> **Note**
>
> Las métricas medidas por eventos de envío de correo electrónico pueden no coincidir totalmente con sus cuotas de envío. Esta discrepancia puede estar causada por rebotes y rechazos de correo electrónico o por el uso del simulador de bandeja de correo de Amazon SES. Para saber lo cerca que está de sus cuotas de envío, consulte Monitoreo de las cuotas de envío.

Para obtener información acerca de cómo utilizar cada método de monitoreo, consulte los siguientes temas:

- Monitoreo de sus estadísticas de envío utilizando la consola de Amazon SES
- Monitoreo de sus estadísticas de uso mediante la API de Amazon SES
- Monitoreo del envío de correo electrónico mediante la publicación de eventos de Amazon SES

Monitoreo de sus estadísticas de envío utilizando la consola de Amazon SES

Desde las páginas Panel de la cuenta, Métricas de reputación y Configuración de SMTP de la consola de Amazon SES, puede monitorear todos sus envíos de correo electrónico, uso, estadísticas, configuración de SMTP, estado general de la cuenta y métricas de reputación. En las secciones siguientes se describen las métricas y estadísticas que se proporcionan en cada una de estas páginas de la consola.

Debe tenerse en cuenta que aunque las páginas de la consola de the section called “Panel de cuenta” y the section called “Métricas de reputación” contienen métricas de rebotes y reclamaciones, hay una sutil diferencia entre cada uno de estos dos conjuntos de tasas de rebote y de reclamaciones, como se explica a continuación:

- Página del panel de la cuenta: en función del intervalo de fechas seleccionado, puede ver cuáles fueron las tasas de rebote y reclamos en el pasado que muestran la progresión de la métrica del cambio previo al presente.
- Página de métricas de reputación: tasas de rebotes y reclamaciones basadas en el último punto de datos recibido al calcular el promedio histórico global a un nivel alto (esto no se debe confundir con la tasa regular de rebotes o reclamaciones, que corresponde a eventos precisos de rebotes o reclamaciones, tal como se muestra en la página del Account dashboard [Panel de la cuenta]).

Como ejemplo sencillo para comparar las tasas de rebote o de reclamaciones entre la página de Reputation metrics (Métricas de reputación) y la página del Account dashboard (Panel de la cuenta), digamos que la tasa fue del 2 % ayer y ahora es del 1 %, en la página de Reputation metrics (Métricas de reputación), solo verá la tasa actual del 1 %, pero en la página del Account dashboard (Panel de la cuenta), los gráficos representarán la progresión trazada que muestra una tasa del 2 % para ayer y del 1 % para hoy.

Panel de cuenta

Puede monitorear el número de correos electrónicos enviados desde la cuenta, así como el porcentaje de la cuota de envío que se ha utilizado, directamente desde la página del Account dashboard (Panel de la cuenta) de la consola de SES en el panel Daily email usage (Uso diario del correo electrónico). Las tasas de entrega y de rechazo de la cuenta se pueden monitorear en el panel Envío de estadísticas, así como otros factores clave relacionados con el envío de correo electrónico en los siguientes paneles:

- Límites de envío: contiene las siguientes cuotas aplicables al envío de correo electrónico a través de SES:
  - Cuota de envío diaria: el número máximo de correos electrónicos que puede enviar en un periodo de 24 horas.
  - Velocidad máxima de envío: el número máximo de correos electrónicos que se puede enviar desde la cuenta por segundo.
- Estado de la cuenta: el estado de la cuenta de SES:
  - `Healthy`: no hay problemas relacionados con la reputación que afecten actualmente a la cuenta.
  - `Under review`: se han identificado problemas potenciales con la cuenta de SES, la cuenta se está revisando mientras trabaja para corregir los problemas.
  - `Paused`: la capacidad de la cuenta para enviar correo electrónico actualmente está suspendida debido a un problema con el correo electrónico enviado desde la cuenta. Cuando se haya corregido el problema, puede solicitar que se reanude la capacidad de la cuenta para enviar correo electrónico.
- Uso diario de correo electrónico: para comprobar el uso diario para asegurarse de que no se acerca a los límites de envío:
  - Correos electrónicos enviados: número total de correos electrónicos enviados en un periodo de 24 horas.
  - Envíos restantes: número total de correos electrónicos restantes disponibles para enviarse en un periodo de 24 horas.
  - Cuota de envío utilizada: porcentaje de la cuota de envío diaria utilizada.
- Estadísticas de envío: se compone de gráficos que muestran la progresión de cuatro métricas esenciales en un conjunto de puntos de datos ordenados por horas que representan los valores de un tipo de evento supervisado que produce estadísticas para el intervalo de fechas seleccionado mediante un periodo de agregación de 1 hora. Puede seleccionar un intervalo de datos con valores iniciales desde `Last 1 day` a `Last 14 days` para filtrar los gráficos a continuación:
  - Envíos: la suma de las solicitudes de envío de correo electrónico correctas para el intervalo de fechas seleccionado.
  - Rechazos: tasa media de solicitudes de envío rechazadas por SES en función de `Rejects/Sends * 100` para el intervalo de fechas seleccionado.
  - Rebotes: tasa media derivada de las métricas de reputación del remitente histórico general que muestra la progresión del intervalo de fechas seleccionado.

- Reclamaciones: tasa media derivada de las métricas de reputación del remitente histórico general que muestra la progresión del intervalo de fechas seleccionado.

Cada uno de estos gráficos contiene un botón View in CloudWatch (Ver en CloudWatch) que abrirá la métrica respectiva en la consola de Amazon CloudWatch, lo que permite ver datos detallados, realizar matemáticas métricas personalizadas y la creación de alarmas en CloudWatch.

Métricas de reputación

Además de las tasas de rebote y reclamaciones descritas, la página de Reputation metrics (Métricas de reputación) también proporciona otra visibilidad de alto nivel de los factores clave que afectan a la reputación que constan de los siguientes paneles:

- Resumen: proporciona información general del estado de la reputación.
  - Estado: estado general de la reputación en función de las tasas históricas de rebote y reclamación:
    - `Healthy`: ambas métricas se encuentran dentro de los niveles normales.
    - `Under review`: una o ambas métricas han provocado automáticamente que la cuenta se sitúe en revisión.
    - `At risk`: una o ambas métricas han alcanzado niveles poco saludables y la capacidad de la cuenta para enviar correos electrónicos puede estar en riesgo.
  - Correos electrónicos enviados (últimas 24 horas): el número total de correos electrónicos enviados en un periodo de 24 horas.
  - Envíos restantes: número total de correos electrónicos restantes disponibles para enviarse en un periodo de 24 horas.
  - Cuota de envío utilizada: porcentaje de la cuota de envío diaria utilizada.
- Contenido de la pestaña de nivel de cuenta:
  - Bounce rate (Tasa de rebotes)
    - Estado: indica el estado de la tasa de rebote utilizando los mismos valores que se describen para el panel de resumen.
    - Tasa de rebote histórica: porcentaje de correos electrónicos de la cuenta que dieron como resultado una devolución permanente calculada a partir del promedio histórico global basado en un volumen representativo que representa las prácticas de envío típicas.
  - Complaint rate (Tasa de reclamaciones)

    - Estado: indica el estado de la tasa de reclamación utilizando los mismos valores que se describen para el panel de resumen.
    - Tasa de rebote histórica: porcentaje de correos electrónicos de la cuenta que dieron como resultado que los destinatarios los notifiquen como spam calculado del promedio histórico global en función del volumen representativo de las prácticas de envío típicas.
- Contenido de la pestaña del conjunto de configuración:
  - Reputación por conjunto de configuración
    - Conjunto de configuración: le permite escribir o seleccionar un conjunto de configuración que tenga habilitadas las métricas de reputación para que pueda ver los datos de resumen, rebote y reclamación basados en los correos electrónicos enviados mediante el conjunto de configuración seleccionado. Los paneles resultantes que aparecen después de seleccionar un conjunto de configuración son los mismos que los descritos anteriormente para la página métricas de reputación, excepto que solo se basan en el correo electrónico enviado con el conjunto de configuración seleccionado en comparación con las métricas de envío globales de nivel de cuenta.

Configuración de SMTP

En esta página se enumeran las configuraciones SMTP necesarias para utilizar la interfaz SMTP de Amazon SES, ya sea a través de la API de SES o mediante programación, y se proporcionan enlaces para crear y administrar sus credenciales de SMTP:

- Configuración SMTP: si desea utilizar un lenguaje de programación, servidor de correo electrónico o aplicación habilitados para SMTP para conectarse a la interfaz SMTP de Amazon SES, se proporciona la siguiente información:
  - Punto de enlace de SMTP
  - Puerto STARTTLS
  - Transport Layer Security (TLS)
  - Puerto de contenedor TLS
  - Enlaces de autenticación proporcionados para la creación y la administración de credenciales de SMTP e IAM

Uso de la consola para monitorear las métricas de envío y reputación

Los siguientes procedimientos le permitirán comenzar a explorar las métricas de envío y reputación mediante la página del Account dashboard (Panel de cuenta) para las métricas basadas en el historial reciente (hasta 14 días) o utilizar la página de Reputation metrics (Métricas de reputación) para obtener métricas basadas en el historial general hasta el momento actual.

Para ver los correos electrónicos enviados y la cuota de envío utilizada

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación, elija Account dashboard (Panel de la cuenta). Las estadísticas de uso se muestran en la sección Daily email usage (Uso diario de correo electrónico).

Para ver el recuento de envíos, tasas de rechazos, rebotes y reclamos

1. En el panel de navegación, elija Account dashboard (Panel de la cuenta).
2. En la sección Sending Statistics (Estadístics de envío), utilice el menú desplegable Date range (Intervalo de fechas) a fin de seleccionar un valor inicial para un intervalo de fechas y filtrar los cuatro gráficos directamente debajo de la sección Sending statistics (Estadísticas de envío).
3. En función del intervalo de fechas seleccionado, puede ver cuáles fueron las tasas de rebote y reclamos en el pasado que muestran la progresión de la métrica del cambio previo al presente.
4. En cualquiera de las tablas, elija el botón View in CloudWatch (Ver en CloduWatch) para abrir la métrica respectiva en la consola de Amazon CloudWatch donde puede ver datos detallados, realizar matemáticas de métricas personalizadas y crear alarmas de supervisión en CloudWatch.

Para consultar las tasas de rebotes y reclamaciones históricas

1. En el panel de navegación, elija Reputation metrics (Métricas de reputación).
2. En el panel Bounce rate (Tasa de rebotes) puede ver el porcentaje de correos electrónicos enviados desde la cuenta que han dado lugar a un rechazo permanente y en Complaint rate (Tasa de reclamaciones) puede consultar el porcentaje de correos electrónicos enviados desde la cuenta que han dado lugar a que los destinatarios los notifiquen como spam; ambas métricas se calculan a partir de un volumen representativo de correo electrónico basado en las prácticas de envío típicas.

3. En cualquiera de los paneles, elija el botón View in CloudWatch (Ver en CloduWatch) para abrir la métrica respectiva en la consola de Amazon CloudWatch donde puede ver datos detallados, realizar matemáticas de métricas personalizadas y crear alarmas de supervisión en CloudWatch.

Para consultar las métricas de reputación por conjuntos de configuración

1. En el panel de navegación, elija Reputation metrics (Métricas de reputación).
2. En la página de métricas de reputación, seleccione la pestaña Configuration set (Conjunto de configuración).
3. En el panel Reputation by configuration set (Reputación por conjunto de configuración), haga clic dentro del Configuration set (Conjunto de configuración) y comience a escribir o seleccione un conjunto de configuración que tenga habilitadas las métricas de reputación.
4. Después de seleccionar el conjunto de configuración, cargará los paneles de resumen, rebote y reclamación que muestran métricas basadas solo en el correo electrónico enviado con el conjunto de configuración seleccionado.

Monitoreo de sus estadísticas de uso mediante la API de Amazon SES

La API de Amazon SES proporciona la operación `GetSendStatistics`, que devuelve información acerca del uso que se hace del servicio. Le recomendamos que compruebe las estadísticas de envío con regularidad, a fin de que pueda realizar ajustes si es necesario.

Si llama a la operación `GetSendStatistics`, recibe una lista de puntos de datos que representan las dos últimas semanas de su actividad de envío. Cada punto de datos de esta lista representa 15 minutos de actividad y contiene la siguiente información para ese periodo:

- El número de rebotes permanentes
- El número de reclamaciones
- El número de intentos de entrega (corresponde al número de correos electrónicos que haya enviado)
- El número de intentos de envío rechazados
- Una marca de tiempo para el periodo de análisis

Para obtener una descripción completa de la operación `GetSendStatistics`, consulte la Referencia de la API de Amazon Simple Email Service.

En esta sección, encontrará los temas siguientes:

- the section called “Llamada a la operación `GetSendStatistics` de la API mediante la AWS CLI”
- the section called “Llamada a la operación `GetSendStatistics` mediante programación”

Llamada a la operación **`GetSendStatistics`** de la API mediante la AWS CLI

La forma más sencilla de llamar a la operación `GetSendStatistics` de la API consiste en utilizar la AWS Command Line Interface (AWS CLI).

Para llamar a la operación **`GetSendStatistics`** de la API utilizando la AWS CLI

1. Si aún no lo ha hecho, descargue e instale la AWS CLI. Para obtener más información, consulte "Instalación de la AWS Command Line Interface" en la Guía del usuario de la AWS Command Line Interface.
2. Si aún no lo ha hecho, configure AWS CLI para utilizar sus credenciales de AWS. Para obtener más información, consulte "Configuración de la AWS CLI" en la Guía del usuario de la AWS Command Line Interface.
3. En la línea de comandos, ejecute el comando siguiente:

   ```
   aws ses get-send-statistics
   ```

   Si la AWS CLI está configurada correctamente, verá una lista de estadísticas de envío en formato JSON. Cada objeto JSON incluye estadísticas de envío agregadas para un periodo de 15 minutos.

Llamada a la operación **`GetSendStatistics`** mediante programación

También puede llamar a la operación `GetSendStatistics` utilizando los SDK de AWS. Esta sección incluye ejemplos de código para los SDK de AWS para Go, PHP, Python y Ruby. Elija uno de los siguientes enlaces para ver ejemplos de código para dicho lenguaje:

- Ejemplo de código para el AWS SDK for Go

- Ejemplo de código para el AWS SDK for PHP
- Ejemplo de código para el AWS SDK for Python (Boto)
- Ejemplo de código para el AWS SDK for Ruby

> **Note**
>
> Estos ejemplos de código suponen que ha creado un archivo de credenciales compartidas de AWS que contiene su ID de clave de acceso de AWS, su clave de acceso secreta de AWS y su región de AWS preferida. Para obtener más información, consulte Archivos de configuración y credenciales compartidas.

Llamada a la **`GetSendStatistics`** mediante AWS SDK for Go

```
package main

import (
    "fmt"

    //go get github.com/aws/aws-sdk-go/...
    "github.com/aws/aws-sdk-go/aws"
    "github.com/aws/aws-sdk-go/aws/session"
    "github.com/aws/aws-sdk-go/service/ses"
    "github.com/aws/aws-sdk-go/aws/awserr"
)

const (
    // Replace us-west-2 with the AWS Region you're using for Amazon SES.
    AwsRegion = "us-west-2"
)

func main() {

    // Create a new session and specify an AWS Region.
    sess, err := session.NewSession(&aws.Config{
        Region:aws.String(AwsRegion)},
    )

    // Create an SES client in the session.
    svc := ses.New(sess)
```

```
    input := &ses.GetSendStatisticsInput{}

    result, err := svc.GetSendStatistics(input)

    // Display error messages if they occur.
    if err != nil {
        if aerr, ok := err.(awserr.Error); ok {
            switch aerr.Code() {
            default:
                fmt.Println(aerr.Error())
            }
        } else {
            // Print the error, cast err to awserr.Error to get the Code and
            // Message from an error.
            fmt.Println(err.Error())
        }
        return
    }

    fmt.Println(result)
}
```

Llamada a la **`GetSendStatistics`** mediante AWS SDK for PHP

```
<?php

// Replace path_to_sdk_inclusion with the path to the SDK as described in
// http://docs.aws.amazon.com/aws-sdk-php/v3/guide/getting-started/basic-usage.html
define('REQUIRED_FILE','path_to_sdk_inclusion');

// Replace us-west-2 with the AWS Region you're using for Amazon SES.
define('REGION','us-west-2');

require REQUIRED_FILE;

use Aws\Ses\SesClient;

$client = SesClient::factory(array(
    'version'=> 'latest',
    'region' => REGION
));

try {
```

```
    $result = $client->getSendStatistics([]);
  echo($result);
} catch (Exception $e) {
    echo($e->getMessage()."\n");
}

?>
```

Llamada a la **GetSendStatistics** mediante AWS SDK for Python (Boto)

```
import boto3 #pip install boto3
import json
from botocore.exceptions import ClientError

client = boto3.client('ses')

try:
    response = client.get_send_statistics(
)
except ClientError as e:
    print(e.response['Error']['Message'])
else:
    print(json.dumps(response, indent=4, sort_keys=True, default=str))
```

Llamada a la **GetSendStatistics** mediante AWS SDK for Ruby

```
require 'aws-sdk' # gem install aws-sdk
require 'json'

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

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

begin

  resp = ses.get_send_statistics({
  })
  puts JSON.pretty_generate(resp.to_h)

# If something goes wrong, display an error message.
```

```
rescue Aws::SES::Errors::ServiceError => error
  puts error

end
```

Monitoreo del envío de correo electrónico mediante la publicación de eventos de Amazon SES

Para que pueda realizar un seguimiento detallado de sus envíos de correo electrónico, puede configurar Amazon SES para que publique los eventos de envío de correos electrónicos a Amazon CloudWatch, Amazon Data Firehose, Amazon Pinpoint o Amazon Simple Notification Service en función de las características que defina.

Puede realizar un seguimiento de varios tipos de eventos de envío de correo electrónico, incluidos envíos, entregas, aperturas, clics, rebotes, quejas, rechazos, fallos de representación y retrasos en la entrega. Esta información puede resultar útil para fines operativos y de análisis. Por ejemplo, puede publicar sus datos de envío de correo electrónico CloudWatch y crear paneles que hagan un seguimiento del rendimiento de sus campañas de correo electrónico, o puede utilizar Amazon SNS para enviarle notificaciones cuando se produzcan determinados eventos.

Cómo funciona la publicación de eventos con los conjuntos de configuración y las etiquetas de los mensajes

Para utilizar la publicación de eventos, primero debe configurar uno o varios conjuntos de configuración. Un conjunto de configuración especifica dónde publicar los eventos y qué eventos publicar. A continuación, cada vez que envíe un correo electrónico, proporcione el nombre del conjunto de configuración y una o varias etiquetas de mensajes, en forma de pares nombre/valor, para clasificar el correo electrónico. Por ejemplo, si promociona libros, puede denominar una etiqueta del mensaje como género y asignarle un valor de ciencia ficción o western, cuando envíe un correo electrónico para la campaña asociada.

Según la interfaz de envío de correo electrónico que utilice, puede proporcionar la etiqueta del mensaje como parámetro del `EmailTags`campo de la operación de la `SendEmail`API o añadir la etiqueta del mensaje al encabezado del correo electrónico específico de SES. `X-SES-MESSAGE-TAGS` Para obtener más información acerca de los conjuntos de configuración, consulte Uso de conjuntos de configuración en Amazon SES.

Además de las etiquetas de mensajes que especifique, Amazon SES también agrega etiquetas automáticas a los mensajes que envía. No necesita realizar ningún paso adicional para utilizar etiquetas automáticas.

En la siguiente tabla se muestran las etiquetas automáticas que se aplican automáticamente a los mensajes que envía con Amazon SES.

Etiquetas automáticas de Amazon SES

Nombre de etiqueta automática	Descripción
`ses:caller-identity`	La identidad de IAM del usuario de Amazon SES que ha enviado el correo electrónico.
`ses:configuration-set`	El nombre del conjunto de configuración asociado al correo electrónico.
`ses:from-domain`	El dominio de la dirección del remitente ("From").
`ses:outgoing-ip`	La dirección IP que Amazon SES utilizó para enviar el correo electrónico.
`ses:source-ip`	La dirección IP que el intermediario utilizó para enviar el correo electrónico.
`ses:source-tls-version`	La versión del protocolo TLS que el intermedi ario usó para enviar el correo electrónico.

Comentarios detallados para las campañas de correo electrónico

La `ses:feedback-id-<a or b>` etiqueta es una etiqueta de mensaje opcional que se puede considerar una etiqueta híbrida o semiautomática. Si bien es similar a las etiquetas automáticas descritas en la sección anterior, la diferencia es que debe agregarla manualmente y usar la clave de prefijo. `ses:` Puedes usar hasta dos de estas etiquetas definidas como y. `ses:feedback-id-a` `ses:feedback-id-b`

Al especificar estas etiquetas, SES las agrega automáticamente al `Feedback-ID` encabezado estándar que se utiliza para proporcionar estadísticas de entrega, como las tasas de quejas y spam, como parte de un ciclo de retroalimentación (FBL), consulte. Bucles de retroalimentación El

`Feedback-ID` encabezado está compuesto por el identificador SESInternalID, utilizado por SES para recopilar información sobre las quejas, y la etiqueta estática, AmazonSES, que identifica a SES como la plataforma de envío, por ejemplo:

`FeedBackId:feedback-id-a:feedback-id-b:((SESInternalID):(AmazonSES))`

Estas etiquetas de identificación de comentarios opcionales se ofrecen como una forma de generar comentarios detallados, como los mensajes que envía como parte de una campaña de correo electrónico. Puedes utilizarla `ses:feedback-id-<a or b>` especificándola como una etiqueta de mensaje en el `EmailTags`campo de la solicitud de `SendEmail`operación, como se muestra en el siguiente ejemplo:

```
{
  "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 lo envía en formato RAW, debe añadirlo `ses:feedback-id-<a or b>` como etiqueta de mensaje al encabezado específico del SES. `X-SES-MESSAGE-TAGS`

La etiqueta de `ses:feedback-id-<a or b>` mensaje también se puede rastrear en Amazon CloudWatch especificándola como fuente de CloudWatch valor como cualquier otra etiqueta de mensaje, consulte the section called “Añadir detalles CloudWatch del destino del evento” (Se aplican cargos adicionales, consulte Precio por métrica para) CloudWatch.

Cómo utilizar la publicación de eventos

Las siguientes secciones contienen la información que tiene que configurar y utilizar la publicación de eventos de Amazon SES.

- Configuración de la publicación de eventos
- Trabajar con datos de eventos

Terminología de publicación de eventos

La siguiente lista define términos relacionados con la publicación de eventos de Amazon SES.

Evento de envío de correo electrónico

La información asociada con el resultado de un correo electrónico que envía a Amazon SES. Los eventos de envío incluyen lo siguiente:

- Send (Envío): la solicitud de envío se realizó de forma correcta y Amazon SES intentará entregar el mensaje al servidor de correo del destinatario. (Si se está utilizando la supresión global o de nivel de cuenta, SES lo seguirá contando como un envío, pero la entrega se suprimirá).
- RenderingFailure— El correo electrónico no se envió debido a un problema de representación de la plantilla. Este tipo de evento se puede producir cuando faltan datos en la plantilla o cuando los parámetros y los datos de la plantilla no coinciden. (Este tipo de evento solo se produce cuando envía correo electrónico con las operaciones de la API `SendTemplatedEmail` o `SendBulkTemplatedEmail`).

- Reject (Rechazo): Amazon SES aceptó el correo electrónico, pero determinó que contenía un virus y no intentó entregarlo al servidor de correo del destinatario.
- Delivery (Entregados): Amazon SES entregó correctamente el correo electrónico al servidor de correo del destinatario.
- Rebotar: una devolución permanente que el servidor de correo del destinatario ha rechazado el correo electrónico de forma permanente. (Los rebotes temporales solo se incluyen cuando Amazon SES no puede entregar el correo electrónico tras intentarlo durante un periodo de tiempo).
- Complaint (Reclamo): el correo electrónico se entregó correctamente al servidor de correo del destinatario, pero el destinatario lo marcó como spam.
- DeliveryDelay— No se pudo entregar el correo electrónico al servidor de correo del destinatario porque se produjo un problema temporal. Pueden producirse retrasos en la entrega, por ejemplo, si la bandeja de entrada del destinatario está llena o el servidor de recepción de email experimenta un problema transitorio.
- Subscriptions (Suscripciones): el correo electrónico se entregó correctamente, pero el destinatario actualizó las preferencias de suscripción al hacer clic en `List-Unsubscribe` en el encabezado del correo electrónico o el enlace `Unsubscribe` del pie de página.
- Open (Abiertos): el destinatario recibió el mensaje y lo abrió en su cliente de correos electrónicos.
- Clic: el destinatario hizo clic en uno o varios enlaces incluidos en el correo electrónico.

Conjunto de configuración

Conjunto de reglas que define el destino en el que Amazon SES publica los eventos de envío de correo electrónico y los tipos de eventos de envío de correo electrónico que desea publicar. Cuando envíe un correo electrónico que desea utilizar con la publicación de eventos, especifique el conjunto de configuración que asociar con el correo electrónico.

Destino de eventos

Un AWS servicio en el que publicas eventos de envío de correos electrónicos de Amazon SES. Cada destino de eventos que configure pertenece a uno y solo a un conjunto de configuración.

Etiqueta de mensajes

Un par nombre/valor que utiliza para clasificar un correo electrónico para fines de publicación de eventos. Los ejemplos son campaña/libro y campaña/ropa. Cuando envía un correo electrónico, especifica la etiqueta del mensaje como parámetro en la llamada a la API o como encabezado de correo electrónico específico de Amazon SES.

Etiqueta automática

Las etiquetas de mensajes que se incluyen automáticamente en informes de publicación de eventos. Hay una etiqueta automática para el nombre del conjunto de configuración, el dominio de la dirección “From”, la dirección IP de salida del intermediario, la dirección IP saliente de Amazon SES y la identidad de IAM del intermediario.

Configuración de publicación de eventos de Amazon SES

En esta sección, se describe lo que debe hacer para configurar Amazon SES de forma que publique los eventos de envío de correo electrónico en los eventos de AWS siguientes:

- Amazon CloudWatch
- Amazon Data Firehose
- Amazon Pinpoint
- Amazon Simple Notification Service (Amazon SNS)

Los siguientes pasos necesarios para configurar la publicación de eventos se tratan en los siguientes temas:

1. Debe crear un conjunto de configuración a través del API o de la consola de Amazon SES.
2. Agregue uno o más destinos del evento (FirehoseCloudWatch, Pinpoint o SNS) al conjunto de configuraciones y configure los parámetros exclusivos del destino del evento.
3. Especifique un conjunto de configuración que contenga su destino de eventos cuando envíe un correo electrónico.

Temas de esta sección

- Paso 1: crear un conjunto de configuración
- Paso 2: añadir un destino de evento
- Paso 3: Especifique el conjunto de configuración cuando envía correo electrónico

Paso 1: crear un conjunto de configuración

Primero debe tener un conjunto de configuración para configurar la publicación de eventos. Si aún no tiene un conjunto de configuración o desea crear uno nuevo, consulte . Creación de conjuntos de configuración en SES

También puede crear conjuntos de configuración mediante la operación CreateConfigurationSet en la API V2 de Amazon SES o la CLI v2 de Amazon SES. Para ello, consulte Cree un conjunto de configuración (AWS CLI).

Paso 2: añadir un destino de evento

Los destinos de eventos son lugares en los que publica eventos de Amazon SES. Cada destino de eventos que configure pertenece a uno y solo a un conjunto de configuración. Cuando configura un destino de evento con Amazon SES, elige el destino del AWS servicio y especifica los parámetros asociados a ese destino.

Al configurar un destino para eventos, puede elegir enviar los eventos a uno de los siguientes AWS servicios:

- Amazon CloudWatch
- Amazon Data Firehose
- Amazon EventBridge
- Amazon Pinpoint
- Amazon Simple Notification Service (Amazon SNS)

El destino de eventos que elija depende del nivel de detalle que desea sobre los eventos y la forma en que desea recibir la información del evento. Si simplemente quieres un total acumulado de cada tipo de evento (por ejemplo, para poder configurar una alarma cuando el total sea demasiado alto), puedes usar CloudWatch.

Si quieres registros de eventos detallados que puedas enviar a otro servicio, como Amazon OpenSearch Service o Amazon Redshift, para su análisis, puedes usar Firehose.

Si desea recibir notificaciones cuando se producen determinados eventos, puede usar Amazon SNS.

Esta sección contiene los siguientes temas

- Configurar un destino de CloudWatch evento para la publicación de eventos

- Configure un destino de eventos de Data Firehose para la publicación de eventos de Amazon SES
- Configura un EventBridge destino de Amazon para la publicación de eventos
- Configuración de un destino de eventos de Amazon Pinpoint para la publicación de eventos
- Configuración de un destino de eventos de Amazon SNS para la publicación de eventos

Configurar un destino de CloudWatch evento para la publicación de eventos

Con CloudWatch las métricas de Amazon, puedes usar los destinos de los eventos para publicar los eventos de envío de correos electrónicos de Amazon SES CloudWatch. Como el destino de un CloudWatch evento solo se puede configurar en un conjunto de configuraciones, primero debe crear un conjunto de configuración y, a continuación, añadir el destino del evento al conjunto de configuraciones.

Al añadir un destino de CloudWatch eventos a un conjunto de configuraciones, debe elegir una o más CloudWatch dimensiones que se correspondan con las etiquetas de los mensajes que utiliza al enviar los correos electrónicos. Al igual que las etiquetas de los mensajes, una CloudWatch dimensión es un par de nombre/valor que le ayuda a identificar una métrica de forma única.

Por ejemplo, podría tener una etiqueta de mensajes y una dimensión denominada `campaign` que usa para identificar su campaña de correo electrónico. Cuando publicas tus eventos de envío de correo electrónico CloudWatch, es importante elegir las etiquetas y dimensiones de los mensajes, ya que estas elecciones afectan a tu CloudWatch facturación y determinan cómo puedes filtrar los datos de los eventos de envío de correo electrónico. CloudWatch

En esta sección se proporciona información que le ayudará a elegir las dimensiones y, a continuación, se muestra cómo añadir un destino de CloudWatch evento a un conjunto de configuraciones.

Temas de esta sección

- Añadir un destino de eventos de CloudWatch
- Selección de CloudWatch dimensiones

Añadir un destino de eventos de CloudWatch

El procedimiento de esta sección muestra cómo añadir los detalles del destino CloudWatch del evento a un conjunto de configuraciones y supone que ha completado los pasos 1 a 6 que se indican más adelanteCrear un destino de eventos.

También puede usar la operación UpdateConfigurationSetEventDestination en la API V2 de Amazon SES para crear y modificar los destinos de los eventos.

Para añadir los detalles CloudWatch del destino del evento a un conjunto de configuraciones mediante la consola

1. Estas son las instrucciones detalladas para seleccionar CloudWatch el tipo de destino del evento en el paso 7 y se supone que ha completado todos los pasos anterioresCrear un destino de eventos. Tras seleccionar el tipo de CloudWatch destino, introducir un nombre de destino y activar la publicación de eventos, se muestra el panel de CloudWatch dimensiones de Amazon, cuyos campos se abordan en los siguientes pasos. (Se aplican cargos adicionales; consulte el precio por métrica para ver.) CloudWatch
2. En Value Source, especifique cómo obtendrá Amazon SES los datos a los que pasa CloudWatch. Están disponibles los siguientes orígenes de valores:

   - Message Tag (Etiqueta de mensaje): Amazon SES recupera el nombre y el valor de la dimensión de una etiqueta que especifica utilizando el encabezado `X-SES-MESSAGE-TAGS` o el parámetro de la API `EmailTags`. Para obtener más información acerca del uso de etiquetas de mensaje, consulte the section called “Paso 3: Especifique el conjunto de configuración al enviar correos”.

     > **Note**
     >
     > Las etiquetas de mensaje pueden incluir los números del 0 al 9, las letras de la A a la Z (mayúsculas y minúsculas), guiones (-) y guiones bajos (_).

     También puede utilizar la fuente del valor Message Tag (Etiqueta de mensaje) para crear dimensiones basadas en las etiquetas automáticas de Amazon SES. Para utilizar una etiqueta automática, escriba el nombre completo de la etiqueta automática como Dimension Name (Nombre de dimensión). Por ejemplo, para crear una dimensión en función de la etiqueta automática del conjunto de configuración, utilice `ses:configuration-set` para el Dimension Name (Nombre de dimensión) y el nombre del conjunto de configuración para el Default Value (Valor predeterminado). Para obtener una lista completa de etiquetas automáticas, consulte Cómo funciona la publicación de eventos con los conjuntos de configuración y las etiquetas de los mensajes.

- Email Header (Encabezado de correo electrónico): Amazon SES recupera el nombre y el valor de la dimensión a partir de un encabezado de correo electrónico.

> **Note**
>
> No puede usar ninguno de los siguientes encabezados de correo electrónico como Dimension Name: `Received`, `To`, `From`, `DKIM-Signature`, `CC`, `message-id` o `Return-Path`.

- Link Tag (Etiqueta de enlace): Amazon SES recupera el nombre y el valor de la dimensión a partir de una etiqueta especificada en un enlace. Para obtener más información sobre cómo añadir etiquetas a los enlaces, consulte ¿Puedo etiquetar enlaces con identificadores únicos?.

3. En Nombre de dimensión, escriba el nombre de la dimensión a la que desea pasar CloudWatch.

> **Note**
>
> Los nombres de dimensión deben contener únicamente letras ASCII (a-z, A-Z), números (0 a 9), guiones bajos (_) y guiones (-). Los espacios, los caracteres acentuados, los caracteres no latinos y otros caracteres especiales no están permitidos.

4. Para Default Value (Valor predeterminado), escriba el valor de la dimensión.

> **Note**
>
> Los valores de dimensión solo deben contener letras ASCII (a-z, A-Z), números (0-9), guiones bajos (_), guiones (-), arrobas (@) y puntos (.). Los espacios, los caracteres acentuados, los caracteres no latinos y otros caracteres especiales no están permitidos.

5. Si desea añadir más dimensiones, elija Add Dimension (Añadir dimensión). En caso contrario, elija Siguiente.
6. En la pantalla de revisión, si está satisfecho con la forma en que ha definido el destino de eventos, elija Add destination (Agregar destino).

Selección de CloudWatch dimensiones

Al elegir nombres y valores para usarlos como CloudWatch dimensiones, tenga en cuenta los siguientes factores:

- Precio por métrica: puedes ver las métricas básicas de Amazon SES de forma CloudWatch gratuita. Sin embargo, si recopila métricas mediante la publicación de eventos, incurre en costos de monitoreo CloudWatch detallado. Cada combinación única de tipo de evento, nombre de dimensión y valor de dimensión crea una métrica diferente. CloudWatch Cuando utilizas CloudWatch Detailed Monitoring, se te cobra por cada métrica. Por este motivo, es posible que desee evitar elegir dimensiones que puedan tener muchos valores diferentes. Por ejemplo, a menos que esté muy interesado en el seguimiento de los eventos de envío de correo electrónico desde el dominio del remitente (“From”), es posible que no desee definir una dimensión para la etiqueta automática de Amazon SES `ses:from-domain`, ya que puede tener muchos valores distintos. Para más información, consulte Precios de CloudWatch.
- Filtrado de métricas: si una métrica tiene varias dimensiones, no puede acceder a la métrica en CloudWatch función de cada dimensión por separado. Por ese motivo, piénselo detenidamente antes de añadir más de una dimensión a un único destino de CloudWatch evento. Por ejemplo, si desea métricas por `campaign` y por una combinación de `campaign` y `genre`, tiene que añadir dos destinos de evento: uno solo con `campaign` como dimensión y otro con `campaign` y `genre` como dimensiones.
- Fuente de los valores de las dimensiones: como alternativa a especificar los valores de las dimensiones utilizando encabezados específicos de Amazon SES o un parámetro para la API, también puede especificar que Amazon SES tome los valores de las dimensiones de sus propios encabezados de mensaje MIME. Podría utilizar esta opción si ya está utilizando encabezados personalizados y no desea cambiar sus mensajes de correo electrónico o sus llamadas a la API de envío de correo electrónico para recopilar métricas en función de los valores de encabezado. Si utiliza sus propios encabezados de mensaje MIME para la publicación de eventos de Amazon SES, los nombres y los valores de los encabezados usados con esta finalidad para Amazon SES solo pueden incluir las letras de la A a la Z, los números del 0 al 9, guiones bajos (_), signos arroba (@), guiones (-) y puntos (.). Si especificas un nombre o un valor que contenga otros caracteres, la llamada de envío del correo electrónico seguirá siendo correcta, pero las estadísticas del evento no se enviarán a Amazon CloudWatch.

Para obtener más información sobre CloudWatch los conceptos, consulta Amazon CloudWatch Concepts en la Guía del CloudWatch usuario de Amazon.

Configure un destino de eventos de Data Firehose para la publicación de eventos de Amazon SES

El destino de un evento de Amazon Data Firehose representa a una entidad que publica eventos específicos de envío de correos electrónicos de Amazon SES a Firehose. Como el destino de un evento Firehose solo se puede configurar en un conjunto de configuraciones, primero hay que

crear un conjunto de configuraciones. A continuación, agregue el destino del evento al conjunto de configuración.

El procedimiento de esta sección muestra cómo añadir los detalles del destino del evento Firehose a un conjunto de configuraciones y se supone que ha completado los pasos del 1 al 6. Crear un destino de eventos

También puede usar la operación UpdateConfigurationSetEventDestination en el destino de la API V2 de Amazon SES para crear y actualizar los destinos de los eventos.

Para añadir los detalles del destino del evento Firehose a un conjunto de configuración mediante la consola

1. Estas son las instrucciones detalladas para seleccionar Firehose como tipo de destino del evento en el paso 7 y se supone que ha completado todos los pasos anteriores. Crear un destino de eventos Tras seleccionar el tipo de destino Firehose, introducir un nombre de destino y activar la publicación de eventos, se muestra el panel de flujo de entrega de Amazon Data Firehose, cuyos campos se abordan en los siguientes pasos.
2. Para la transmisión de entrega, selecciona una transmisión de Firehose existente o selecciona Crear nueva transmisión para crear una nueva con la consola de Firehose.

   Para obtener información sobre la creación de una transmisión mediante la consola Firehose, consulte Creación de una transmisión de entrega de Amazon Kinesis Firehose en la Guía para desarrolladores de Amazon Data Firehose.
3. Para el rol de Identity and Access Management (IAM), elija un rol de IAM para el que Amazon SES tenga permiso para publicar en Firehose en su nombre. Puede elegir un rol existente, hacer que Amazon SES cree un rol para usted o crear su propio rol.

   Si eliges un rol existente o creas el tuyo propio, debes modificar manualmente las políticas del rol para dar permiso al rol para acceder a la transmisión de entrega de Firehose y para dar permiso a Amazon SES para asumir el rol. Para ver ejemplos de políticas, consulte Otorgar permiso a Amazon SES para publicar en tu Firehose Delivery Stream.
4. Elija Siguiente.
5. En la pantalla de revisión, si está satisfecho con la forma en que ha definido el destino de eventos, elija Add destination (Agregar destino).

Para obtener información sobre cómo usar la `UpdateConfigurationSetEventDestination` API para añadir un destino de eventos de Firehose, consulta la referencia de la API de Amazon Simple Email Service.

Otorgar permiso a Amazon SES para publicar en tu Firehose Delivery Stream

Para permitir que Amazon SES publique registros en su transmisión de entrega de Firehose, debe usar un rol AWS Identity and Access Management (IAM) y adjuntar o modificar la política de permisos y la política de confianza del rol. La política de permisos permite que la función publique registros en su transmisión de entrega de Firehose, y la política de confianza permite que Amazon SES asuma esa función.

En esta sección, se proporcionan ejemplos de ambas políticas. Para obtener más información acerca de cómo adjuntar políticas a roles de IAM, consulte Modificación de un rol en la Guía del usuario de IAM.

Política de permisos

La siguiente política de permisos permite que el rol publique registros de datos en su transmisión de entrega de Firehose.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Action": [
        "firehose:PutRecordBatch"
      ],
      "Resource": [
        "arn:aws:firehose:delivery-region:111122223333:deliverystream/delivery-stream-name"
      ]
    }
  ]
}
```

En la política de ejemplo anterior, realice los siguientes cambios:

- Sustituya *la región de entrega por* la AWS región en la que creó la transmisión de entrega de Firehose.

- Reemplace *111122223333* por su ID de cuenta de AWS .
- Sustituya el *nombre del flujo de entrega por el nombre* del flujo de entrega de Firehose.

Política de confianza

La siguiente política de confianza habilita a Amazon SES para que asuma el rol.

```
{
  "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"
        }
      }
    }
  ]
}
```

En la política de ejemplo anterior, realice los siguientes cambios:

- Sustituya *la región de entrega por* la AWS región en la que creó la transmisión de entrega de Firehose.
- Reemplace *111122223333* por su ID de cuenta de AWS .
- Sustituya *configuration-set-name* por el nombre del conjunto de configuración asociado al flujo de entrega de Firehose.

Configura un EventBridge destino de Amazon para la publicación de eventos

Un destino de EventBridge eventos de Amazon te notifica los eventos de envío de correo electrónico que especifiques en un conjunto de configuraciones. SES genera y envía los eventos de envío de correos electrónicos al bus de eventos EventBridge predeterminado. Un bus de eventos es un router que recibe eventos y puede entregarlos a varios destinos. Puedes obtener más información sobre la integración de eventos de envío de correo electrónico con Amazon EventBridge enMonitorización mediante EventBridge. Como el destino de un EventBridge evento solo se puede configurar en un conjunto de configuraciones, debe crear un conjunto de configuración antes de añadir el destino del evento al conjunto de configuraciones.

En el procedimiento de esta sección se muestra cómo agregar los detalles EventBridge del destino del evento a un conjunto de configuración y se supone que ha completado los pasos 1 a 6 descritos más abajoCrear un destino de eventos.

También puede usar la operación UpdateConfigurationSetEventDestination en la API V2 de Amazon SES para crear y modificar los destinos de los eventos.

Para añadir los detalles EventBridge del destino del evento a un conjunto de configuraciones mediante la consola

1. Estas son las instrucciones detalladas para seleccionar EventBridge el tipo de destino del evento en el paso 7 y se supone que ha completado todos los pasos anterioresCrear un destino de eventos. Tras seleccionar el tipo de EventBridge destino de Amazon, introducir un nombre de destino y activar la publicación de eventos, se mostrará un panel informativo sobre el autobús de EventBridge eventos de Amazon.
2. Elija Siguiente.
3. En la pantalla de revisión, si está satisfecho con la forma en que ha definido el destino de eventos, elija Add destination (Agregar destino). Se abrirá la página de resumen del destino del evento en la que un banner de éxito confirmará si el destino del evento se ha creado o modificado en forma correcta.

Configuración de un destino de eventos de Amazon Pinpoint para la publicación de eventos

El destino de un evento de Amazon Pinpoint le notifica los eventos de envío de correo electrónico que especifique en un conjunto de configuraciones. Como el destino de un evento de Amazon Pinpoint solo se puede configurar en un conjunto de configuraciones, debe crear un conjunto de configuración antes de añadir el destino del evento al conjunto de configuraciones.

En el procedimiento de esta sección se muestra cómo agregar detalles de destino de eventos de Amazon Pinpoint a un conjunto de configuración y se supone que ha completado los pasos del 1 al 6 de Crear un destino de eventos.

También puede usar la operación UpdateConfigurationSetEventDestination en la API V2 de Amazon SES para crear y modificar los destinos de los eventos.

Hay cargos adicionales por los tipos de canales que haya configurado en sus proyectos de Amazon Pinpoint. Para obtener más información, consulte Precios de Amazon Pinpoint.

Para agregar detalles del destino de eventos de Amazon Pinpoint a un conjunto de configuración mediante la consola

1. Estas son las instrucciones detalladas para seleccionar Amazon Pinpoint como tipo de destino de evento en Paso 7 y supone que ha completado todos los pasos anteriores en Crear un destino de eventos.

   > **Note**
   >
   > Amazon Pinpoint no admite los tipos de eventos Delivery delays (Retrasos de entrega) ni Subscriptions (Suscripciones).

   Tras seleccionar el tipo de destino de Amazon Pinpoint, introducir un nombre de destino y activar la publicación de eventos, aparece el panel de detalles del proyecto de Amazon Pinpoint, cuyos campos se abordan en los siguientes pasos.

2. En Project (Proyecto), elija un proyecto existente de Amazon Pinpoint o elija Create a new project in Amazon Pinpoint (Crear un nuevo proyecto en Amazon Pinpoint) para crear uno nuevo.

   Para obtener información sobre la creación de un proyecto, consulte Crear un proyecto en la Guía del usuario de Amazon Pinpoint.

3. Elija Siguiente.

4. En la pantalla de revisión, si está satisfecho con la forma en que ha definido el destino de eventos, elija Add destination (Agregar destino). Se abrirá la página de resumen del destino del evento en la que un banner de éxito confirmará si el destino del evento se ha creado o modificado en forma correcta.

Configuración de un destino de eventos de Amazon SNS para la publicación de eventos

Un destino de eventos de Amazon SNS le notifica los eventos de envío de correo electrónico que especifique en un conjunto de configuraciones. Como el destino de un evento de Amazon SNS solo se puede configurar en un conjunto de configuración, debe crear un conjunto de configuración antes de añadir el destino del evento al conjunto de configuraciones.

En el procedimiento de esta sección se muestra cómo agregar detalles de destino de eventos de Amazon SNS a un conjunto de configuración y se supone que ha completado los pasos del 1 al 6 de Crear un destino de eventos.

También puede usar la operación UpdateConfigurationSetEventDestination en la API V2 de Amazon SES para crear y modificar los destinos de los eventos.

> **Note**
>
> Las notificaciones de feedback sobre devoluciones, quejas y entregas también se pueden configurar a través de Amazon SNS para cualquiera de las identidades de envío verificadas. Para obtener más información, consulte the section called “Configuración de notificaciones de Amazon SNS”.

Se aplican cargos adicionales por enviar mensajes a los puntos de enlace que están suscritos a sus temas de Amazon SNS. Para obtener más información, consulte Precios de Amazon SNS.

Para agregar detalles del destino de eventos de Amazon SNS a un conjunto de configuración mediante la consola

1. Estas son las instrucciones detalladas para seleccionar Amazon SNS como tipo de destino de evento en Paso 7 y supone que ha completado todos los pasos anteriores en Crear un destino de eventos. Tras seleccionar el tipo de destino de Amazon SNS, introducir un nombre de destino y activar la publicación de eventos, aparece el panel de temas de Amazon Simple Notification Service (SNS), cuyos campos se abordan en los siguientes pasos.
2. Para SNS Topic (Tema de SNS), elija un tema de Amazon SNS existente o elija Create SNS topic (Crear tema de SNS) para crear uno nuevo.

   Para obtener más información acerca de la creación de un tema, consulte Creación de un tema en la Guía para desarrolladores de Amazon Simple Notification Service.

> **Important**
>
> Al crear un tema con Amazon SNS, en Type (Tipo), solo elija Standard (Estándar). (SES no admite temas de tipo FIFO).

3. Elija Siguiente.
4. En la pantalla de revisión, si está satisfecho con la forma en que ha definido el destino de eventos, elija Add destination (Agregar destino). Se abrirá la página de resumen del destino del evento en la que un banner de éxito confirmará si el destino del evento se ha creado o modificado en forma correcta.
5. Tanto si creó un nuevo tema de SNS como si seleccionó uno existente, ahora deberá conceder acceso a SES para publicar notificaciones sobre el tema. En la página de resumen del destino del evento del paso anterior, elija Amazon SNS desde la columna Destination type (Tipo de destino); esto lo dirigirá a la lista Topics (Temas) en la consola de Amazon Simple Notification Service, realice los siguientes pasos desde la consola de Amazon SNS:

   a. Seleccione el nombre del tema de SNS que creó o modificó en el paso anterior.
   b. En la pantalla de detalles del tema, elija Edit (Editar).
   c. Para conceder permiso a SES para publicar notificaciones sobre el tema, en la pantalla Edit topic (Editar tema) de la consola de SNS, expanda Access policy (Política de acceso) y en el JSON editor (Editor de JSON), agregue la siguiente política de permisos:

```
{
  "Version": "2012-10-17",
  "Id": "notification-policy",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ses.amazonaws.com"
      },
      "Action": "sns:Publish",
      "Resource": "arn:aws:sns:topic_region:111122223333:topic_name",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "111122223333",
```

```
          "AWS:SourceArn":
 "arn:aws:ses:topic_region:111122223333:configuration-set/configuration-set-
name"
        }
      }
    }
  ]
}
```

En la política de ejemplo anterior, realice los siguientes cambios:

- Reemplace *topic_region* por la región de AWS en la que creó el tema de SNS.
- Sustituya *111122223333* por el ID de su cuenta. AWS
- Reemplace *topic_name* por el nombre del tema de SNS.
- Reemplace *configuration-set-name* por el nombre del conjunto de configuración asociado al destino de eventos de SNS.

d. Elija Guardar cambios.

Paso 3: Especifique el conjunto de configuración cuando envía correo electrónico

Después de crear un conjunto de configuración y añadir un evento de destino, el último paso para la publicación de eventos consiste en enviar sus mensajes de correo electrónico.

Para publicar eventos asociados con un correo electrónico, debe proporcionar el nombre del conjunto de configuración para asociar con el correo electrónico. Opcionalmente, puede proporcionar etiquetas de mensaje para categorizar el correo electrónico.

Debe proporcionar esta información a Amazon SES como parámetros para la API de envío de correo electrónico, encabezados de correo electrónico específicos de Amazon SES o encabezados personalizados en el mensaje MIME. El método que elija depende de la interfaz de envío de correo electrónico que utilice, tal y como se muestra en la siguiente tabla.

Interfaz de envío de correo electrónico	Formas de publicar eventos
`SendEmail`	Parámetros de la API
`SendTemplatedEmail`	Parámetros de la API

Interfaz de envío de correo electrónico	Formas de publicar eventos
`SendBulkTemplatedEmail`	Parámetros de la API
`SendCustomVerificationEmail`	Parámetros de la API
`SendRawEmail`	Parámetros de la API, encabezados de correo electrónico específicos de Amazon SES o encabezados MIME personalizados **Important** Si especifica etiquetas de mensajes utilizando ambos encabezados y parámetros de la API, Amazon SES utiliza solo las etiquetas de mensajes proporcionadas por los parámetro s de la API. Amazon SES no une etiquetas de mensajes especificadas por encabezados y parámetros de la API.
Interfaz de SMTP	Encabezados de correo electrónico específicos de Amazon SES

En las secciones siguientes se describe cómo especificar el conjunto de configuración y las etiquetas de mensajes utilizando encabezados y utilizando parámetros de la API.

- Uso de parámetros de la API de Amazon SES
- Uso de encabezados de correo electrónico específicos de Amazon SES
- Uso de encabezados de correo electrónico personalizados

> **Note**
>
> También puede incluir etiquetas de mensaje en los encabezados de los correos electrónicos. Las etiquetas de mensaje pueden incluir los números del 0 al 9, las letras de la A a la Z (mayúsculas y minúsculas), guiones (-) y guiones bajos (_).

Uso de parámetros de la API de Amazon SES

Para utilizar SendEmail, SendTemplatedEmail, SendBulkTemplatedEmail, SendCustomVerificationEmail o SendRawEmail con la publicación de eventos, debe especificar el conjunto de configuraciones y las etiquetas de mensajes mediante la transferencia de estructuras de datos denominadas ConfigurationSet y MessageTag a la llamada a la API.

Para obtener más información acerca del uso de la API de Amazon SES, consulte la Referencia de la API de Amazon Simple Email Service.

Uso de encabezados de correo electrónico específicos de Amazon SES

Cuando utilice `SendRawEmail` o la interfaz de SMTP, para especificar el conjunto de configuración y las etiquetas de mensajes, puede agregar encabezados específicos de Amazon SES al correo electrónico. Amazon SES elimina los encabezados antes de enviar el correo electrónico. En la siguiente tabla se muestran los nombres de los encabezados que utilizar.

Información de publicación de eventos	Encabezado
Conjunto de configuración	`X-SES-CONFIGURATION-SET`
Etiquetas de mensajes	`X-SES-MESSAGE-TAGS`

En el siguiente ejemplo se muestra el aspecto que podrían tener los encabezados en un correo electrónico sin procesar que envíe a 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--
```

Uso de encabezados de correo electrónico personalizados

Aunque debe especificar el nombre del conjunto de configuración utilizando el encabezado `X-SES-CONFIGURATION-SET` específico de Amazon SES, puede especificar las etiquetas de mensajes utilizando sus propios encabezados MIME.

> **Note**
>
> Los nombres y valores de encabezado que utilice para la publicación de eventos de Amazon SES deben estar en ASCII. Si especifica un valor o un nombre de encabezado no ASCII para la publicación de eventos de Amazon SES, la llamada de envío de correo electrónico seguirá realizándose correctamente, pero las métricas del evento no se emitirán a Amazon CloudWatch.

Trabajar con datos de eventos de Amazon SES

Después de configurar la publicación de eventos y especificar un conjunto de configuración para el envío de correos electrónicos, puede recuperar los eventos de envío de correo electrónico desde el destino de eventos especificado al configurar el conjunto de configuración asociado con el correo electrónico.

En esta sección se describe cómo recuperar los eventos de envío de correo electrónico de Amazon CloudWatch y Amazon Data Firehose, y cómo interpretar los datos de eventos proporcionados por Amazon SNS.

- Recuperación de datos de eventos de Amazon SES desde CloudWatch

- Recuperación de datos de eventos de Amazon SES de Firehose
- Interpretación de datos de eventos de Amazon SES desde Amazon SNS

Recuperación de datos de eventos de Amazon SES desde CloudWatch

Puede publicar las siguientes métricas de envío de correo de Amazon SES en Amazon CloudWatch. Al publicar datos de eventos en CloudWatch, proporciona estas métricas como un conjunto ordenado de datos de series temporales. Puede utilizar estas métricas para monitorizar el rendimiento de su envío de correo electrónico. Por ejemplo, puede monitorear la métrica de reclamos y establecer una alarma de CloudWatch que se desencadene cuando la métrica supere un determinado valor.

Hay dos niveles de grado de detalle con los que Amazon SES puede publicar estos eventos en CloudWatch:

- En su Cuenta de AWS: estas métricas amplias, que corresponden a las métricas que monitorea con la consola de Amazon SES y la API de `GetSendStatistics`, son totales en toda su Cuenta de AWS. Amazon SES publica estas métricas en CloudWatch automáticamente.
- Detalladas: estas métricas se clasifican por características de email que define mediante etiquetas de mensajes. Para publicar estas métricas en CloudWatch, debe configurar la publicación de eventos con un destino de eventos de CloudWatch y especificar un conjunto de configuración al enviar un correo electrónico. También puede especificar etiquetas de mensajes o utilizar las etiquetas automáticas que Amazon SES proporciona de forma automática.

En esta sección, se describen las métricas disponibles y cómo ver las métricas en CloudWatch.

Métricas disponibles

Puede publicar las siguientes métricas de envío de correo de Amazon SES en CloudWatch:

- Send (Envío): la solicitud de envío se realizó de forma correcta y Amazon SES intentará entregar el mensaje al servidor de correo del destinatario. (Si se está utilizando la supresión global o de nivel de cuenta, SES lo seguirá contando como un envío, pero la entrega se suprimirá).
- RenderingFailure: no se envió el correo electrónico debido a un problema con la presentación de la plantilla. Este tipo de evento se puede producir cuando faltan datos en la plantilla o cuando los parámetros y los datos de la plantilla no coinciden. (Este tipo de evento solo se produce cuando envía correo electrónico con las operaciones de la API `SendTemplatedEmail` o `SendBulkTemplatedEmail`).

- Reject (Rechazo): Amazon SES aceptó el correo electrónico, pero determinó que contenía un virus y no intentó entregarlo al servidor de correo del destinatario.
- Delivery (Entregados): Amazon SES entregó correctamente el correo electrónico al servidor de correo del destinatario.
- Rebotar: una devolución permanente que el servidor de correo del destinatario ha rechazado el correo electrónico de forma permanente. (Los rebotes temporales solo se incluyen cuando Amazon SES no puede entregar el correo electrónico tras intentarlo durante un periodo de tiempo).
- Complaint (Reclamo): el correo electrónico se entregó correctamente al servidor de correo del destinatario, pero el destinatario lo marcó como spam.
- DeliveryDelay: el correo electrónico no se pudo entregar al servidor de correo del destinatario porque se produjo un problema temporal. Pueden producirse retrasos en la entrega, por ejemplo, si la bandeja de entrada del destinatario está llena o el servidor de recepción de email experimenta un problema transitorio.
- Subscriptions (Suscripciones): el correo electrónico se entregó correctamente, pero el destinatario actualizó las preferencias de suscripción al hacer clic en `List-Unsubscribe` en el encabezado del correo electrónico o el enlace `Unsubscribe` del pie de página.
- Open (Abiertos): el destinatario recibió el mensaje y lo abrió en su cliente de correos electrónicos.
- Clic: el destinatario hizo clic en uno o varios enlaces incluidos en el correo electrónico.

Dimensiones disponibles

CloudWatch utiliza los nombres de dimensiones que se especifican al agregar un evento de destino de CloudWatch a un conjunto de configuración en Amazon SES. Para obtener más información, consulte Configurar un destino de CloudWatch evento para la publicación de eventos.

Visualización de métricas de Amazon SES en la consola de CloudWatch

El siguiente procedimiento describe cómo ver las métricas de publicación de eventos de Amazon SES utilizando la consola de CloudWatch.

Para ver las métricas a través de la consola de CloudWatch

1. Inicie sesión en la AWS Management Console y abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. Si es necesario, cambie la región. En la barra de navegación, seleccione la región donde residen sus recursos de AWS. Para obtener más información, consulte Regiones y puntos de enlace.

3. En el panel de navegación, seleccione Todas las métricas.
4. En el panel Métricas, seleccione SES.
5. Elija la métrica que desea ver. Para ver métricas de publicación de eventos detalladas, elija la combinación de dimensiones que especificó al configurar el destino de eventos de CloudWatch. Para obtener más información sobre la visualización de métricas con CloudWatch, consulte Use Amazon CloudWatch metrics (Uso de las métricas de Amazon CloudWatch).

Para ver métricas mediante la AWS CLI

- En el símbolo del sistema, ejecute el siguiente comando:

```
aws cloudwatch list-metrics --namespace "AWS/SES"
```

Recuperación de datos de eventos de Amazon SES de Firehose

Amazon SES publica los eventos de envío de correos electrónicos a Firehose como registros JSON. A continuación, Firehose publica los registros en el destino de AWS servicio que eligió al configurar el flujo de entrega en Firehose. Para obtener información sobre cómo configurar los flujos de entrega de Firehose, consulte Creación de un flujo de entrega de Firehose en la Guía para desarrolladores de Amazon Data Firehose.

Temas de esta sección:

- Contenido de los datos de eventos que Amazon SES publica en Firehose
- Ejemplos de datos de eventos que Amazon SES publica en Firehose

Contenido de los datos de eventos que Amazon SES publica en Firehose

Amazon SES publica los registros de eventos de envío de correos electrónicos a Amazon Data Firehose en formato JSON. Al publicar eventos en Firehose, Amazon SES sigue cada registro JSON con un carácter de nueva línea.

Puede encontrar registros de ejemplo para todos estos tipos de notificación en Ejemplos de datos de eventos que Amazon SES publica en Firehose.

Temas de esta sección

- Objeto JSON de nivel superior

- Objeto Mail
- Objeto Bounce
- Objeto Complaint
- Objeto Delivery
- Objeto Send
- Objeto Reject
- Objeto Open
- Objeto Click
- Objeto Rendering Failure
- DeliveryDelay objeto
- Objeto suscripción

Objeto JSON de nivel superior

El objeto JSON de nivel superior en un registro de eventos de envío de correo electrónico contiene los siguientes campos.

Nombre del campo	Descripción
`eventType`	Una cadena que describe el tipo de evento. Valores posibles: `Bounce`, `Complaint` , `Delivery`, `Send`, `Reject`, `Open`, `Click`, `Rendering Failure`, `DeliveryDelay` o `Subscription` . Si no configuró la publicación de eventos este campo se denomina `notificationType` .
`mail`	Un objeto JSON que contiene información acerca del mensaje de correo electrónico que produjo el evento.
`bounce`	Este campo solo está presente si `eventType` es `Bounce`. Contiene información sobre el rebote.

Nombre del campo	Descripción
`complaint`	Este campo solo está presente si `eventType` es `Complaint` . Contiene información sobre la reclamación.
`delivery`	Este campo solo está presente si `eventType` es `Delivery`. Contiene información sobre la entrega.
`send`	Este campo solo está presente si `eventType` es `Send`.
`reject`	Este campo solo está presente si `eventType` es `Reject`. Contiene información sobre el rechazo.
`open`	Este campo solo está presente si `eventType` es `Open`. Contiene información sobre el evento de apertura.
`click`	Este campo solo está presente si `eventType` es `Click`. Contiene información sobre el evento de clic.
`failure`	Este campo solo está presente si `eventType` es `Rendering Failure` . Contiene información sobre el evento de error de presentación.
`deliveryDelay`	Este campo solo está presente si `eventType` es `DeliveryDelay` . Contiene información sobre el retraso en la entrega de un correo electrónico.
`subscription`	Este campo solo está presente si `eventType` es `Subscription` . Contiene información sobre las preferencias de suscripción.

Objeto Mail

Cada registro de evento de envío de correo electrónico contiene información acerca del correo electrónico original en el objeto `mail`. El objeto JSON que contiene información acerca de un objeto `mail` tiene los campos siguientes.

Nombre del campo	Descripción
`timestamp`	La fecha y la hora, en formato ISO8601 (AAAA-MM-DDThh:mm:ss.sZ), en la que se envió el mensaje.
`messageId`	Un ID exclusivo que Amazon SES asignó al mensaje. Amazon SES le devolvió este valor cuando envió el mensaje. **Note** Este ID de mensaje lo asignó Amazon SES. Puede encontrar el ID de mensaje del correo electrónico original en los campos `headers` y `commonHeaders` del objeto `mail`.
`source`	La dirección de correo electrónico desde la que se envió el mensaje (la dirección MAIL FROM del sobre).
`sourceArn`	El nombre de recurso de Amazon (ARN) de la identidad que se utilizó para enviar el correo electrónico. En el caso de una autorización de envío, el `sourceArn` es el ARN de la identidad que el propietario de la identidad autorizó utilizar al remitente delegado para enviar el correo electrónico. Para obtener más información acerca de la autorización de envío,

Nombre del campo	Descripción
	consulte Métodos de autenticación del correo electrónico.
`sendingAccountId`	El ID de cuenta de AWS de la cuenta que se utilizó para enviar el correo electrónico. En el caso de la autorización de envío, el `sendingAccountId` es el ID de cuenta del remitente delegado.
`destination`	Una lista de direcciones de correo electrónico que han sido destinatarios del correo electrónico original.
`headersTruncated`	Una cadena que especifica si los encabezados están truncados en la notificación, que se produce si los encabezados tienen un tamaño superior a 10 KB. Los posibles valores son `true` y `false`.
`headers`	Una lista de los encabezados originales del correo electrónico. Cada encabezado de la lista tiene un campo `name` y un campo `value`. **Note** Cualquier ID de mensaje dentro del campo `headers` procede del mensaje original que pasó a Amazon SES. El ID de mensaje que Amazon SES asignó seguidamente al mensaje está en el campo `messageId` del objeto `mail`.

Nombre del campo	Descripción
`commonHeaders`	Un mapeo de los encabezados originales del correo electrónico utilizados habitualmente. **Note** El ID de mensaje dentro del campo `commonHeaders` es el ID de mensaje que Amazon SES asignó seguidamente al mensaje en el campo `messageId` del objeto `mail`.
`tags`	Una lista de etiquetas asociadas al correo electrónico.

Objeto Bounce

El objeto JSON que contiene información acerca de un evento `Bounce` tendrá siempre los campos siguientes.

Nombre del campo	Descripción
`bounceType`	El tipo de rebote, tal como determina Amazon SES.
`bounceSubType`	El subtipo de rebote, tal como determina Amazon SES.
`bouncedRecipients`	Una lista que contiene información acerca de los destinatarios del mensaje de correo electrónico original que dio lugar a un rebote.
`timestamp`	La fecha y la hora, en formato ISO8601 (AAAA-MM-DDThh:mm:ss.sZ), a la que el ISP envió la notificación de rebote.

Nombre del campo	Descripción
`feedbackId`	Un ID único para el rebote.
`reportingMTA`	El valor del campo `Reporting-MTA` del DSN. Se trata del valor de la autoridad de transfere ncia de mensajes (MTA) que intentó realizar la operación de entrega, retransmisión o gateway descrita en el DSN. **Note** Este campo solo aparece si se ha adjuntado una notificación de estado de entrega (DSN) al rebote.

Destinatarios con rebote

Un evento de rebote podría pertenecer a un único destinatario o a varios destinatarios. El campo `bouncedRecipients` aloja una lista de objetos (un objeto por destinatario a quien pertenece el evento de rebote) y siempre contendrá el campo siguiente.

Nombre del campo	Descripción
`emailAddress`	La dirección de correo electrónico del destinata rio. Si hay un DSN disponible, se trata del valor del campo `Final-Recipient` del DSN.

Opcionalmente, si hay un DSN adjunto al rebote, los siguientes campos también podrían estar presentes.

Nombre del campo	Descripción
`action`	El valor del campo `Action` del DSN. Esto indica la acción que realiza el MTA de notificac

Nombre del campo	Descripción
	ión como resultado de su intento de entregar el mensaje a este destinatario.
`status`	El valor del campo `Status` del DSN. Se trata del código de estado independiente del transporte por destinatario que indica el estado de entrega del mensaje.
`diagnosticCode`	El código de estado emitido por la MTA de notificación. Este es el valor del campo `Diagnostic-Code` del DSN. Este campo puede estar ausente en el DSN (y, por lo tanto, también ausente en el JSON).

Tipos de rebote

Cada evento se rebote será uno de los tipos que se muestra en la tabla siguiente.

El sistema de publicación de eventos solo publica rechazos permanentes y rebotes temporales que Amazon SES ya no volverá a intentar. Si recibe rebotes marcados como `Permanent`, debería eliminar las direcciones de correo electrónico correspondientes de su lista de correo, ya que no podrá enviar mensajes a estas en el futuro. Los rebotes `Transient` se le envían cuando un mensaje ha tenido un rebote temporal varias veces y Amazon SES ha dejado de intentar volver a enviarlo. Es posible que en el futuro pueda volver a enviar correctamente a una dirección que inicialmente ha dado lugar a un rebote `Transient`.

bounceType	bounceSubType	Descripción
`Undetermined`	`Undetermined`	Amazon SES no ha podido determinar un motivo específico de rebote.
`Permanent`	`General`	Amazon SES recibió un rechazo permanente general. Si recibe este tipo de rebote, debería eliminar la dirección de correo electrónico del destinatario de su lista de correo.

bounceType	bounceSubType	Descripción
`Permanent`	`NoEmail`	Amazon SES recibió un rechazo permanent e porque la dirección de correo electrónico de destino no existe. Si recibe este tipo de rebote, debería eliminar la dirección de correo electróni co del destinatario de su lista de correo.
`Permanent`	`Suppressed`	Amazon SES ha suprimido el envío a esta dirección dado que tiene un historial reciente de rebotes como dirección no válida. Para anular la lista de supresión global, consulte Uso de la lista de supresión de nivel de cuenta de Amazon SES.
`Permanent`	`OnAccountSuppressi onList`	Amazon SES ha suprimido el envío a esta dirección porque está en la lista de supresión de nivel de cuenta. Esto no se toma en cuenta para calcular la métrica de porcentaje de rebotes.
`Transient`	`General`	Amazon SES recibió un rebote general. Es posible que pueda enviar correctamente a este destinatario en el futuro.
`Transient`	`MailboxFull`	Amazon SES ha recibido un rebote completo de bandeja de entrada. Es posible que pueda enviar correctamente a este destinatario en el futuro.
`Transient`	`MessageTooLarge`	Amazon SES recibió un rebote de mensaje demasiado grande. Es posible que pueda enviar correctamente a este destinatario si reduce el tamaño del mensaje.

bounceType	bounceSubType	Descripción
`Transient`	`ContentRejected`	Amazon SES ha recibido un rebote de contenido rechazado. Es posible que pueda enviar correctamente a este destinatario si cambia el contenido del mensaje.
`Transient`	`AttachmentRejected`	Amazon SES ha recibido un rebote de archivo adjunto rechazado. Es posible que pueda enviar correctamente a este destinatario si elimina o cambia el archivo adjunto.

Objeto Complaint

El objeto JSON que contiene información acerca de un evento `Complaint` tiene los campos siguientes.

Nombre del campo	Descripción
`complainedRecipients`	Una lista que contiene información sobre destinatarios que podrían haber enviado la reclamación.
`timestamp`	La fecha y la hora, en formato ISO8601 (AAAA-MM-DDThh:mm:ss.sZ), a la que el ISP envió la notificación de reclamación.
`feedbackId`	Un ID único para el reclamo.
`complaintSubType`	El subtipo del reclamo, tal como determina Amazon SES.

Además, si se adjunta un informe de retroalimentación a la reclamación, podrían estar presentes los siguientes campos.

Nombre del campo	Descripción
`userAgent`	El valor del campo `User-Agent` del informe de retroalimentación. Esto indica el nombre y la versión del sistema que generó el informe.
`complaintFeedbackType`	El valor del campo `Feedback-Type` del informe de retroalimentación recibido desde el ISP. Contiene el tipo de retroalimentación.
`arrivalDate`	El valor del campo `Arrival-Date` o `Received-Date` del informe de retroalimentación en formato ISO8601 (AAAA-MM-DDThh:mm:ss.sZ). Este campo puede estar ausente en el informe (y, por lo tanto, también ausente en el JSON).

Destinatarios con reclamaciones

El campo `complainedRecipients` contiene una lista de destinatarios que podrían haber enviado la reclamación.

> **Important**
>
> Dado que la mayoría de los ISP redactan la dirección de correo electrónico del destinatario que presentó el reclamo desde su notificación de reclamo, esta lista contiene información acerca de los destinatarios que podrían haber enviado el reclamo, en función de los destinatarios del mensaje original y el ISP desde el que hemos recibido el reclamo. Amazon SES realiza una búsqueda en el mensaje original para determinar esta lista de destinatarios.

Los objetos JSON de esta lista contienen el siguiente campo.

Nombre del campo	Descripción
`emailAddress`	La dirección de correo electrónico del destinatario.

Tipos de reclamación

Es posible que vea los siguientes tipos de reclamación en el campo `complaintFeedbackType` tal como los ha asignado el ISP que realiza la notificación, de acuerdo con el sitio web de Internet Assigned Numbers Authority:

Nombre del campo	Descripción
`abuse`	Indica correo electrónico no solicitado o algún otro tipo de abuso de correo electrónico.
`auth-failure`	Informe de error de autenticación de correo electrónico.
`fraud`	Indica algún tipo de fraude o actividad de phishing.
`not-spam`	Indica que la entidad que proporciona el informe no considera el mensaje como spam. Esto se puede utilizar para corregir un mensaje que estaba mal etiquetado o clasificado como spam.
`other`	Indica cualquier otra retroalimentación que no encaje en otros tipos registrados.
`virus`	Notifica que se ha encontrado un virus en el mensaje de origen.

Objeto Delivery

El objeto JSON que contiene información acerca de un evento `Delivery` tendrá siempre los campos siguientes.

Nombre del campo	Descripción
`timestamp`	La fecha y la hora en que Amazon SES entregó el correo electrónico al servidor de correo del

Nombre del campo	Descripción
	destinatario, en formato ISO8601 (AAAA-MM-DDThh:mm:ss.sZ).
`processingTimeMillis`	El tiempo en milisegundos desde el momento en que Amazon SES aceptó la solicitud del remitente hasta el momento en que Amazon SES transfirió el mensaje al servidor de email del destinatario.
`recipients`	Una lista de los destinatarios a los que corresponden los eventos de entrega.
`smtpResponse`	El mensaje de respuesta SMTP del ISP remoto que ha aceptado el correo electrónico desde Amazon SES. Este mensaje variará por email, por receptor de servidor de recepción de email y por ISP de recepción.
`reportingMTA`	El nombre del anfitrión del servidor de email de Amazon SES que envió el email.

Objeto Send

El objeto JSON que contiene información acerca de un evento `send` está siempre vacío.

Objeto Reject

El objeto JSON que contiene información acerca de un evento `Reject` tendrá siempre los campos siguientes.

Nombre del campo	Descripción
`reason`	La razón por la que se rechazó el correo electrónico. El único valor posible es `Bad content`, lo que significa que Amazon SES detectó que el correo electrónico contenía un virus. Cuando se rechaza un mensaje, Amazon

Nombre del campo	Descripción
	SES detiene el procesamiento y no intenta entregarlo al servidor de correo del destinatario.

Objeto Open

El objeto JSON que contiene información acerca de un evento `Open` contendrá siempre los campos siguientes.

Nombre del campo	Descripción
`ipAddress`	La dirección IP del destinatario.
`timestamp`	La fecha y la hora en la que se produjo el evento de apertura del correo electrónico, en formato ISO8601 (AAAA-MM-DDThh:mm:ss.sZ).
`userAgent`	El agente del usuario del dispositivo o cliente de correo electrónico que el destinatario utiliza para abrir el correo electrónico.

Objeto Click

El objeto JSON que contiene información acerca de un evento `Click` contendrá siempre los campos siguientes.

Nombre del campo	Descripción
`ipAddress`	La dirección IP del destinatario.
`timestamp`	La fecha y la hora en la que se produjo el evento de clic, en formato ISO8601 (AAAA-MM-DDThh:mm:ss.sZ).

Nombre del campo	Descripción
`userAgent`	El agente del usuario del cliente que el destinatario usó para hacer clic en un enlace en el correo electrónico.
`link`	La dirección URL del enlace en el que el destinatario hizo clic.
`linkTags`	Una lista de las etiquetas que se añadieron al enlace utilizando el atributo `ses:tags`. Para obtener más información sobre la adición de etiquetas a enlaces en sus correos electróni cos, consulte P5. ¿Puedo etiquetar enlaces con identificadores únicos? en la Preguntas frecuentes sobre métricas de envío de correo electrónico de Amazon SES.

Objeto Rendering Failure

El objeto JSON que contiene información acerca de un evento `Rendering Failure` tiene los campos siguientes.

Nombre del campo	Descripción
`templateName`	El nombre de la plantilla que se usó para enviar el correo electrónico.
`errorMessage`	Un mensaje que proporciona más información sobre el error de presentación.

DeliveryDelay objeto

El objeto JSON que contiene información acerca de un evento `DeliveryDelay` tiene los campos siguientes.

Nombre del campo	Descripción
`delayType`	El tipo de retraso. Los valores posibles son los siguientes: • InternalFailure— Un problema interno de Amazon SES provocó el retraso del mensaje. • General: se produjo un error genérico durante la conversación SMTP. • MailboxFull— El buzón del destinatario está lleno y no puede recibir más mensajes. • SpamDetected— El servidor de correo del destinatario ha detectado una gran cantidad de correo electrónico no solicitado de su cuenta. • RecipientServerError— Un problema temporal con el servidor de correo electróni co del destinatario impide la entrega del mensaje. • IPFailure: el proveedor de correo electrónico del destinatario bloquea o limita la dirección IP que envía el mensaje. • TransientCommunicationFailure— Se produjo un error de comunicación temporal durante la conversación SMTP con el proveedor de correo electrónico del destinata rio. • BYOIP HostNameLookupUnavailable: Amazon SES no pudo buscar el nombre de host DNS de sus direcciones IP. Este tipo de retraso únicamente se produce cuando se utiliza Bring Your Own IP. • Undetermined: Amazon SES no pudo determinar el motivo del retraso en la entrega.

Nombre del campo	Descripción
	• SendingDeferral— Amazon SES ha considerado apropiado aplazar internamente el mensaje.
`delayedRecipients`	Objeto que contiene información sobre el destinatario del correo electrónico.
`expirationTime`	La fecha y hora en que Amazon SES dejará de intentar entregar el mensaje. Este valor se muestra en formato ISO 8601.
`reportingMTA`	La dirección IP del Agente de transferencia de mensajes (MTA) que informó del retraso.
`timestamp`	Fecha y hora en que se produjo el retraso, que se muestra en formato ISO 8601.

Destinatarios con retraso

El objeto `delayedRecipients` contiene los siguientes valores.

Nombre del campo	Descripción
`emailAddress`	La dirección de correo electrónico que provocó el retraso en la entrega del mensaje.
`status`	El código de estado SMTP asociado al retraso de la entrega.
`diagnosticCode`	El código de diagnóstico proporcionado por el agente de transferencia de mensajes (MTA) receptor.

Objeto suscripción

El objeto JSON que contiene información acerca de un evento `Subscription` tiene los campos siguientes.

Nombre del campo	Descripción
`contactList`	El nombre de la lista de contacto está activado.
`timestamp`	La fecha y la hora, en formato ISO8601 (AAAA-MM-DDThh:mm:ss.sZ), cuando el ISP envió la notificación de suscripción.
`source`	La dirección de correo electrónico desde la que se envió el mensaje (la dirección MAIL FROM del sobre).
`newTopicPreferences`	Estructura de datos JSON (mapa) que especific a el estado de suscripción de todos los temas de la lista de contactos que indica el estado después de un cambio (contacto suscrito o cancelado).
`oldTopicPreferences`	Estructura de datos JSON (mapa) que especific a el estado de suscripción de todos los temas de la lista de contactos que indica el estado antes del cambio (contacto suscrito o cancelado).

Preferencias de tema nuevo o antiguo

Los objetos `newTopicPreferences` y `oldTopicPreferences` contienen los siguientes valores.

Nombre del campo	Descripción
`unsubscribeAll`	Especifica si se canceló la suscripción del contacto de todos los temas de la lista de contactos.

Nombre del campo	Descripción
`topicSubscriptionStatus`	Especifica el tema en el `topicName` campo y mapea el estado (OptIno OptOut) de la suscripción en el `subscriptionStatus` campo.
`topicDefaultSubscriptionStatus`	Especifica el tema del `topicName` campo y mapea el estado (OptIno OptOut) de la suscripción en el `subscriptionStatus` campo.

Ejemplos de datos de eventos que Amazon SES publica en Firehose

En esta sección se proporcionan ejemplos de los tipos de registro de eventos de envío de correo electrónico que Amazon SES publica en Firehose.

Temas de esta sección:

- Registro Bounce
- Registro Complaint
- Registro Delivery
- Registro Send
- Registro Reject
- Registro Open
- Registro Click
- Registro Rendering Failure
- DeliveryDelay registro
- Registro de suscripción

> **Note**
>
> En los siguientes ejemplos en los que se utiliza un campo `tag`, se emplea la publicación de eventos a través de un conjunto de configuración para el que SES admite la publicación de etiquetas para todos los tipos de eventos. Si se utilizan las notificaciones de respuesta

directamente en la identidad, SES no publica las etiquetas. Consulte cómo agregar etiquetas al crear un conjunto de configuración o modificar un conjunto de configuración.

Registro Bounce

El siguiente es un ejemplo de un registro de `Bounce` eventos que Amazon SES publica en 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"
      ]
    }
  }
}
```

Registro Complaint

El siguiente es un ejemplo de un registro de `Complaint` eventos que Amazon SES publica en 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"
      ]
    }
  }
}
```

Registro Delivery

El siguiente es un ejemplo de un registro de `Delivery` eventos que Amazon SES publica en Firehose.

```
{
  "eventType": "Delivery",
  "mail": {
```

```
    "timestamp": "2016-10-19T23:20:52.240Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination": [
      "recipient@example.com"
    ],
    "headersTruncated": false,
    "headers": [
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "text/html; charset=UTF-8"
      },
      {
        "name": "Content-Transfer-Encoding",
        "value": "7bit"
      }
    ],
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "to": [
        "recipient@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES"
```

```
    },
    "tags": {
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:caller-identity": [
        "ses_user"
      ],
      "ses:outgoing-ip": [
        "192.0.2.0"
      ],
      "myCustomTag1": [
        "myCustomTagValue1"
      ],
      "myCustomTag2": [
        "myCustomTagValue2"
      ]
    }
  },
  "delivery": {
    "timestamp": "2016-10-19T23:21:04.133Z",
    "processingTimeMillis": 11893,
    "recipients": [
      "recipient@example.com"
    ],
    "smtpResponse": "250 2.6.0 Message received",
    "reportingMTA": "mta.example.com"
  }
}
```

Registro Send

El siguiente es un ejemplo de un registro de `Send` eventos que Amazon SES publica en 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": {}
}
```

Registro Reject

El siguiente es un ejemplo de un registro de `Reject` eventos que Amazon SES publica en 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"
  }
}
```

Registro Open

El siguiente es un ejemplo de un registro de 0pen eventos que Amazon SES publica en Firehose.

```
{
  "eventType": "Open",
  "mail": {
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES",
      "to": [
        "recipient@example.com"
      ]
    },
    "destination": [
      "recipient@example.com"
    ],
    "headers": [
      {
        "name": "X-SES-CONFIGURATION-SET",
        "value": "ConfigSet"
      },
      {
        "name":"X-SES-MESSAGE-TAGS",
        "value":"myCustomTag1=myCustomValue1, myCustomTag2=myCustomValue2"
      },
      {
```

```
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "multipart/alternative; boundary=\"XBoundary\""
      }
    ],
    "headersTruncated": false,
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "sendingAccountId": "123456789012",
    "source": "sender@example.com",
    "tags": {
      "myCustomTag1":[
        "myCustomValue1"
      ],
      "myCustomTag2":[
        "myCustomValue2"
      ],
      "ses:caller-identity": [
        "IAM_user_or_role_name"
      ],
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ]
    },
```

```
    "timestamp": "2017-08-09T21:59:49.927Z"
  },
  "open": {
    "ipAddress": "192.0.2.1",
    "timestamp": "2017-08-09T22:00:19.652Z",
    "userAgent": "Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X)
 AppleWebKit/603.3.8 (KHTML, like Gecko) Mobile/14G60"
  }
}
```

Registro Click

El siguiente es un ejemplo de un registro de `Click` eventos que Amazon SES publica en Firehose.

```
{
  "eventType": "Click",
  "click": {
    "ipAddress": "192.0.2.1",
    "link": "http://docs.aws.amazon.com/ses/latest/DeveloperGuide/send-email-
smtp.html",
    "linkTags": {
      "samplekey0": [
        "samplevalue0"
      ],
      "samplekey1": [
        "samplevalue1"
      ]
    },
    "timestamp": "2017-08-09T23:51:25.570Z",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/60.0.3112.90 Safari/537.36"
  },
  "mail": {
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES",
      "to": [
        "recipient@example.com"
      ]
    },
    "destination": [
```

```
      "recipient@example.com"
    ],
    "headers": [
      {
        "name": "X-SES-CONFIGURATION-SET",
        "value": "ConfigSet"
      },
      {
        "name":"X-SES-MESSAGE-TAGS",
        "value":"myCustomTag1=myCustomValue1, myCustomTag2=myCustomValue2"
      },
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "multipart/alternative; boundary=\"XBoundary\""
      },
      {
        "name": "Message-ID",
        "value": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000"
      }
    ],
    "headersTruncated": false,
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "sendingAccountId": "123456789012",
    "source": "sender@example.com",
    "tags": {
      "myCustomTag1":[
        "myCustomValue1"
      ],
```

```
      "myCustomTag2":[
        "myCustomValue2"
      ],
      "ses:caller-identity": [
        "ses_user"
      ],
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ]
    },
    "timestamp": "2017-08-09T23:50:05.795Z"
  }
}
```

Registro Rendering Failure

El siguiente es un ejemplo de un registro de `Rendering Failure` eventos que Amazon SES publica en Firehose.

```
{
  "eventType":"Rendering Failure",
  "mail":{
    "timestamp":"2018-01-22T18:43:06.197Z",
    "source":"sender@example.com",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "tags":{
      "ses:configuration-set":[
        "ConfigSet"
      ]
    }
  },
```

```
  "failure":{
    "errorMessage":"Attribute 'attributeName' is not present in the rendering data.",
    "templateName":"MyTemplate"
  }
}
```

DeliveryDelay registro

El siguiente es un ejemplo de un registro de `DeliveryDelay` eventos que Amazon SES publica en Firehose.

```
{
  "eventType": "DeliveryDelay",
  "mail":{
    "timestamp":"2020-06-16T00:15:40.641Z",
    "source":"sender@example.com",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "tags":{
      "ses:configuration-set":[
        "ConfigSet"
      ]
    }
  },
  "deliveryDelay": {
    "timestamp": "2020-06-16T00:25:40.095Z",
    "delayType": "TransientCommunicationFailure",
    "expirationTime": "2020-06-16T00:25:40.914Z",
    "delayedRecipients": [{
      "emailAddress": "recipient@example.com",
      "status": "4.4.1",
      "diagnosticCode": "smtp; 421 4.4.1 Unable to connect to remote host"
    }]
  }
}
```

Registro de suscripción

El siguiente es un ejemplo de un registro de `Subscription` eventos que Amazon SES publica en Firehose.


```
{
  "eventType": "Subscription",
  "mail": {
    "timestamp": "2022-01-12T01:00:14.340Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLEe4bccb684-777bc8de-afa7-4970-92b0-f515137b1497-000000",
    "destination": ["recipient@example.com"],
    "headersTruncated": false,
    "headers": [
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "text/html; charset=UTF-8"
      },
      {
        "name": "Content-Transfer-Encoding",
        "value": "7bit"
      }
    ],
    "commonHeaders": {
      "from": ["sender@example.com"],
      "to": ["recipient@example.com"],
```

```
      "messageId": "EXAMPLEe4bccb684-777bc8de-afa7-4970-92b0-f515137b1497-000000",
      "subject": "Message sent from Amazon SES"
    },
    "tags": {
      "ses:operation": ["SendEmail"],
      "ses:configuration-set": ["ConfigSet"],
      "ses:source-ip": ["192.0.2.0"],
      "ses:from-domain": ["example.com"],
      "ses:caller-identity": ["ses_user"],
      "myCustomTag1": ["myCustomValue1"],
      "myCustomTag2": ["myCustomValue2"]
    }
  },
  "subscription": {
    "contactList": "ContactListName",
    "timestamp": "2022-01-12T01:00:17.910Z",
    "source": "UnsubscribeHeader",
    "newTopicPreferences": {
      "unsubscribeAll": true,
      "topicSubscriptionStatus": [
        {
          "topicName": "ExampleTopicName",
          "subscriptionStatus": "OptOut"
        }
      ]
    },
    "oldTopicPreferences": {
      "unsubscribeAll": false,
      "topicSubscriptionStatus": [
        {
          "topicName": "ExampleTopicName",
          "subscriptionStatus": "OptOut"
        }
      ]
    }
  }
}
```

Interpretación de datos de eventos de Amazon SES desde Amazon SNS

Amazon SES publica eventos de envío de correo electrónico en Amazon Simple Notification Service (Amazon SNS) como registros JSON. A continuación, Amazon SNS entrega notificaciones a los puntos de enlace suscritos al tema de Amazon SNS asociado al destino de eventos. Para

obtener información acerca de cómo configurar temas y suscripciones en Amazon SNS, consulte Introducción en la Guía para desarrolladores de Amazon Simple Notification Service.

Para obtener una descripción del contenido de registros y registros de ejemplo, consulte las secciones siguientes.

- Contenido de los registros de eventos
- Ejemplos de registros de evento

Contenido de los datos de eventos que Amazon SES publica en Amazon SNS

Amazon SES publica registros de eventos de envío de correo electrónico en Amazon Simple Notification Service en formato JSON.

Puede encontrar registros de ejemplo para todos estos tipos de notificación en Ejemplos de datos de eventos que Amazon SES publica en Amazon SNS.

Temas de esta sección:

- Objeto JSON de nivel superior
- Objeto Mail
- Objeto Bounce
- Objeto Complaint
- Objeto Delivery
- Objeto Send
- Objeto Reject
- Objeto Open
- Objeto Click
- Objeto Rendering Failure
- Objeto DeliveryDelay
- Objeto suscripción

Objeto JSON de nivel superior

El objeto JSON de nivel superior en un registro de eventos de envío de correo electrónico contiene los siguientes campos. El tipo de evento determina qué otros objetos están presentes.

Nombre del campo	Descripción
`eventType`	Una cadena que describe el tipo de evento. Valores posibles: `Bounce`, `Complaint` , `Delivery`, `Send`, `Reject`, `Open`, `Click`, `Rendering Failure`, `DeliveryDelay` o `Subscription` . Si no configuró la publicación de eventos este campo se denomina `notificationType` .
`mail`	Un objeto JSON que contiene información acerca del mensaje de correo electrónico que produjo el evento.
`bounce`	Este campo solo está presente si `eventType` es `Bounce`. Contiene información sobre el rebote.
`complaint`	Este campo solo está presente si `eventType` es `Complaint` . Contiene información sobre la reclamación.
`delivery`	Este campo solo está presente si `eventType` es `Delivery`. Contiene información sobre la entrega.
`send`	Este campo solo está presente si `eventType` es `Send`.
`reject`	Este campo solo está presente si `eventType` es `Reject`. Contiene información sobre el rechazo.
`open`	Este campo solo está presente si `eventType` es `Open`. Contiene información sobre el evento de apertura.

Nombre del campo	Descripción
`click`	Este campo solo está presente si `eventType` es `Click`. Contiene información sobre el evento de clic.
`failure`	Este campo solo está presente si `eventType` es `Rendering Failure`. Contiene información sobre el evento de error de presentación.
`deliveryDelay`	Este campo solo está presente si `eventType` es `DeliveryDelay`. Contiene información sobre el retraso en la entrega de un correo electrónico.
`subscription`	Este campo solo está presente si `eventType` es `Subscription`. Contiene información sobre las preferencias de suscripción.

Objeto Mail

Cada registro de evento de envío de correo electrónico contiene información acerca del correo electrónico original en el objeto `mail`. El objeto JSON que contiene información acerca de un objeto `mail` tiene los campos siguientes.

Nombre del campo	Descripción
`timestamp`	La fecha y la hora, en formato ISO8601 (AAAA-MM-DDThh:mm:ss.sZ), en la que se envió el mensaje.
`messageId`	Un ID exclusivo que Amazon SES asignó al mensaje. Amazon SES le devolvió este valor cuando envió el mensaje.

Nombre del campo	Descripción
	Note Este ID de mensaje lo asignó Amazon SES. Puede encontrar el ID de mensaje del correo electrónico original en los campos `headers` y `commonHeaders` del objeto `mail`.
`source`	La dirección de correo electrónico desde la que se envió el mensaje (la dirección MAIL FROM del sobre).
`sourceArn`	El nombre de recurso de Amazon (ARN) de la identidad que se utilizó para enviar el correo electrónico. En el caso de una autorización de envío, el `sourceArn` es el ARN de la identidad que el propietario de la identidad autorizó utilizar al remitente delegado para enviar el correo electrónico. Para obtener más información acerca de la autorización de envío, consulte Métodos de autenticación del correo electrónico.
`sendingAccountId`	El ID de cuenta de AWS de la cuenta que se utilizó para enviar el correo electrónico. En el caso de la autorización de envío, el `sendingAccountId` es el ID de cuenta del remitente delegado.
`destination`	Una lista de direcciones de correo electrónico que han sido destinatarios del correo electrónico original.

Nombre del campo	Descripción
`headersTruncated`	Una cadena que especifica si los encabezados están truncados en la notificación, que se produce si los encabezados tienen un tamaño superior a 10 KB. Los posibles valores son `true` y `false`.
`headers`	Una lista de los encabezados originales del correo electrónico. Cada encabezado de la lista tiene un campo `name` y un campo `value`. **Note** Cualquier ID de mensaje dentro del campo `headers` procede del mensaje original que pasó a Amazon SES. El ID de mensaje que Amazon SES asignó seguidamente al mensaje está en el campo `messageId` del objeto `mail`.
`commonHeaders`	Un mapeo de los encabezados originales del correo electrónico utilizados habitualmente. **Note** El ID de mensaje dentro del campo `commonHeaders` es el ID de mensaje que Amazon SES asignó seguidamente al mensaje en el campo `messageId` del objeto `mail`.
`tags`	Una lista de etiquetas asociadas al correo electrónico.

Objeto Bounce

El objeto JSON que contiene información acerca de un evento `Bounce` tiene los campos siguientes.

Nombre del campo	Descripción
`bounceType`	El tipo de rebote, tal como determina Amazon SES.
`bounceSubType`	El subtipo de rebote, tal como determina Amazon SES.
`bouncedRecipients`	Una lista que contiene información acerca de los destinatarios del mensaje de correo electrónico original que dio lugar a un rebote.
`timestamp`	La fecha y la hora, en formato ISO8601 (AAAA-MM-DDThh:mm:ss.sZ), a la que el ISP envió la notificación de rebote.
`feedbackId`	Un ID único para el rebote.
`reportingMTA`	El valor del campo `Reporting-MTA` del DSN. Se trata del valor de la autoridad de transferencia de mensajes (MTA) que intentó realizar la operación de entrega, retransmisión o gateway descrita en el DSN. **Note** Este campo solo aparece si se ha adjuntado una notificación de estado de entrega (DSN) al rebote.

Destinatarios con rebote

Un evento de rebote podría pertenecer a un único destinatario o a varios destinatarios. El campo `bouncedRecipients` incluye una lista de objetos (un objeto por destinatario cuya dirección de correo electrónico produjo un rebote) y contiene el campo siguiente.

Nombre del campo	Descripción
`emailAddress`	La dirección de correo electrónico del destinatario. Si hay un DSN disponible, se trata del valor del campo `Final-Recipient` del DSN.

Opcionalmente, si hay un DSN adjunto al rebote, los siguientes campos también podrían estar presentes.

Nombre del campo	Descripción
`action`	El valor del campo `Action` del DSN. Esto indica la acción que realiza el MTA de notificación como resultado de su intento de entregar el mensaje a este destinatario.
`status`	El valor del campo `Status` del DSN. Se trata del código de estado independiente del transporte por destinatario que indica el estado de entrega del mensaje.
`diagnosticCode`	El código de estado emitido por la MTA de notificación. Este es el valor del campo `Diagnostic-Code` del DSN. Este campo puede estar ausente en el DSN (y, por lo tanto, también ausente en el JSON).

Tipos de rebote

Cada evento de rebote es de uno de los tipos que se muestran en la tabla siguiente.

El sistema de publicación de eventos solo publica rechazos permanentes y rebotes temporales que Amazon SES ya no volverá a intentar. Si recibe rebotes marcados como `Permanent`, debería eliminar las direcciones de correo electrónico correspondientes de su lista de correo, ya que no podrá enviar mensajes a estas en el futuro. Los rebotes `Transient` se le envían cuando un mensaje ha tenido un rebote temporal varias veces y Amazon SES ha dejado de intentar volver a enviarlo. Es posible que en el futuro pueda volver a enviar correctamente a una dirección que inicialmente ha dado lugar a un rebote `Transient`.

bounceType	bounceSubType	Descripción
`Undetermined`	`Undetermined`	Amazon SES no ha podido determinar un motivo específico de rebote.
`Permanent`	`General`	Amazon SES recibió un rechazo permanente general. Si recibe este tipo de rebote, debería eliminar la dirección de correo electrónico del destinatario de su lista de correo.
`Permanent`	`NoEmail`	Amazon SES recibió un rechazo permanente porque la dirección de correo electrónico de destino no existe. Si recibe este tipo de rebote, debería eliminar la dirección de correo electrónico del destinatario de su lista de correo.
`Permanent`	`Suppressed`	Amazon SES ha suprimido el envío a esta dirección dado que tiene un historial reciente de rebotes como dirección no válida. Para anular la lista de supresión global, consulte Uso de la lista de supresión de nivel de cuenta de Amazon SES.
`Permanent`	`OnAccountSuppressionList`	Amazon SES ha suprimido el envío a esta dirección porque está en la lista de supresión de nivel de cuenta. Esto no se toma en cuenta para calcular la métrica de porcentaje de rebotes.

bounceType	bounceSubType	Descripción
`Transient`	`General`	Amazon SES recibió un rebote general. Es posible que pueda enviar correctamente a este destinatario en el futuro.
`Transient`	`MailboxFull`	Amazon SES ha recibido un rebote completo de bandeja de entrada. Es posible que pueda enviar correctamente a este destinatario en el futuro.
`Transient`	`MessageTooLarge`	Amazon SES recibió un rebote de mensaje demasiado grande. Es posible que pueda enviar correctamente a este destinatario si reduce el tamaño del mensaje.
`Transient`	`ContentRejected`	Amazon SES ha recibido un rebote de contenido rechazado. Es posible que pueda enviar correctamente a este destinatario si cambia el contenido del mensaje.
`Transient`	`AttachmentRejected`	Amazon SES ha recibido un rebote de archivo adjunto rechazado. Es posible que pueda enviar correctamente a este destinatario si elimina o cambia el archivo adjunto.

Objeto Complaint

El objeto JSON que contiene información acerca de un evento `Complaint` tiene los campos siguientes.

Nombre del campo	Descripción
`complainedRecipients`	Una lista que contiene información sobre destinatarios que podrían haber enviado la reclamación.

Nombre del campo	Descripción
`timestamp`	La fecha y la hora, en formato ISO8601 (AAAA-MM-DDThh:mm:ss.sZ), a la que el ISP envió la notificación de reclamación.
`feedbackId`	Un ID único para el reclamo.
`complaintSubType`	El subtipo del reclamo, tal como determina Amazon SES.

Además, si se adjunta un informe de retroalimentación a la reclamación, podrían estar presentes los siguientes campos.

Nombre del campo	Descripción
`userAgent`	El valor del campo `User-Agent` del informe de retroalimentación. Esto indica el nombre y la versión del sistema que generó el informe.
`complaintFeedbackType`	El valor del campo `Feedback-Type` del informe de retroalimentación recibido desde el ISP. Contiene el tipo de retroalimentación.
`arrivalDate`	El valor del campo `Arrival-Date` o `Received-Date` del informe de retroalim entación en formato ISO8601 (AAAA-MM-D DThh:mm:ss.sZ). Este campo puede estar ausente en el informe (y, por lo tanto, también ausente en el JSON).

Destinatarios con reclamaciones

El campo `complainedRecipients` contiene una lista de destinatarios que podrían haber enviado la reclamación.

> **Important**
>
> La mayoría de los ISP redactan las direcciones de correo electrónico de los destinatarios que envían reclamaciones. Por este motivo, el campo `complainedRecipients` incluye una lista de todos los destinatarios que han enviado el correo electrónico con una dirección en el dominio que emitió la notificación de reclamación.

Los objetos JSON de esta lista contienen el siguiente campo.

Nombre del campo	Descripción
`emailAddress`	La dirección de correo electrónico del destinatario.

Tipos de reclamación

Es posible que vea los siguientes tipos de reclamación en el campo `complaintFeedbackType` tal como los ha asignado el ISP que realiza la notificación, de acuerdo con el sitio web de Internet Assigned Numbers Authority:

Nombre del campo	Descripción
`abuse`	Indica correo electrónico no solicitado o algún otro tipo de abuso de correo electrónico.
`auth-failure`	Informe de error de autenticación de correo electrónico.
`fraud`	Indica algún tipo de fraude o actividad de phishing.
`not-spam`	Indica que la entidad que proporciona el informe no considera el mensaje como spam. Esto se puede utilizar para corregir un mensaje que estaba mal etiquetado o clasificado como spam.

Nombre del campo	Descripción
`other`	Indica cualquier otra retroalimentación que no encaje en otros tipos registrados.
`virus`	Notifica que se ha encontrado un virus en el mensaje de origen.

Subtipos de reclamaciones

El valor del campo `complaintSubType` puede ser nulo o `OnAccountSuppressionList`. Si el valor es `OnAccountSuppressionList`, Amazon SES aceptó el mensaje, pero no intentó enviarlo porque estaba en la lista de supresión de nivel de cuenta.

Objeto Delivery

El objeto JSON que contiene información acerca de un evento `Delivery` tiene los campos siguientes.

Nombre del campo	Descripción
`timestamp`	La fecha y la hora en que Amazon SES entregó el correo electrónico al servidor de correo del destinatario, en formato ISO8601 (AAAA-MM-DDThh:mm:ss.sZ).
`processingTimeMillis`	El tiempo en milisegundos desde el momento en que Amazon SES aceptó la solicitud del remitente hasta el momento en que Amazon SES transfirió el mensaje al servidor de email del destinatario.
`recipients`	Una lista de los destinatarios a los que corresponden los eventos de entrega.
`smtpResponse`	El mensaje de respuesta SMTP del ISP remoto que ha aceptado el correo electrónico desde Amazon SES. Este mensaje variará por email,

Nombre del campo	Descripción
	por receptor de servidor de recepción de email y por ISP de recepción.
`reportingMTA`	El nombre del anfitrión del servidor de email de Amazon SES que envió el email.

Objeto Send

El objeto JSON que contiene información acerca de un evento `send` está siempre vacío.

Objeto Reject

El objeto JSON que contiene información acerca de un evento `Reject` tiene los campos siguientes.

Nombre del campo	Descripción
`reason`	La razón por la que se rechazó el correo electrónico. El único valor posible es `Bad content`, lo que significa que Amazon SES detectó que el correo electrónico contenía un virus. Cuando se rechaza un mensaje, Amazon SES detiene el procesamiento y no intenta entregarlo al servidor de correo del destinata rio.

Objeto Open

El objeto JSON que contiene información acerca de un evento `Open` tiene los campos siguientes.

Nombre del campo	Descripción
`ipAddress`	La dirección IP del destinatario.
`timestamp`	La fecha y la hora en la que se produjo el evento de apertura del correo electrónico, en

Nombre del campo	Descripción
	formato ISO8601 (AAAA-MM-DDThh:mm:ss.sZ).
`userAgent`	El agente del usuario del dispositivo o cliente de correo electrónico que el destinatario utiliza para abrir el correo electrónico.

Objeto Click

El objeto JSON que contiene información acerca de un evento `Click` tiene los campos siguientes.

Nombre del campo	Descripción
`ipAddress`	La dirección IP del destinatario.
`timestamp`	La fecha y la hora en la que se produjo el evento de clic, en formato ISO8601 (AAAA-MM-DDThh:mm:ss.sZ).
`userAgent`	El agente del usuario del cliente que el destinatario usó para hacer clic en un enlace en el correo electrónico.
`link`	La dirección URL del enlace en el que el destinatario hizo clic.
`linkTags`	Una lista de las etiquetas que se añadieron al enlace utilizando el atributo `ses:tags`. Para obtener más información sobre la adición de etiquetas a enlaces en sus correos electrónicos, consulte P5. ¿Puedo etiquetar enlaces con identificadores únicos? en la Preguntas frecuentes sobre métricas de envío de correo electrónico de Amazon SES.

Objeto Rendering Failure

El objeto JSON que contiene información acerca de un evento `Rendering Failure` tiene los campos siguientes.

Nombre del campo	Descripción
`templateName`	El nombre de la plantilla que se usó para enviar el correo electrónico.
`errorMessage`	Un mensaje que proporciona más información sobre el error de presentación.

Objeto DeliveryDelay

El objeto JSON que contiene información acerca de un evento `DeliveryDelay` tiene los campos siguientes.

Nombre del campo	Descripción
`delayType`	El tipo de retraso. Los valores posibles son los siguientes: • InternalFailure: un problema interno de Amazon SES provocó que el mensaje se retrasara. • General: se produjo un error genérico durante la conversación SMTP. • MailboxFull: el buzón del destinatario está lleno y no puede recibir mensajes adicional es. • SpamDetected: el servidor de correo del destinatario detectó una gran cantidad de correos electrónicos no solicitados de su cuenta.

Nombre del campo	Descripción
	• RecipientServerError: un problema temporal con el servidor de correo electrónico del destinatario impide la entrega del mensaje. • IPFailure: el proveedor de correo electrónico del destinatario bloquea o limita la dirección IP que envía el mensaje. • TransientCommunicationFailure: hubo un error temporal de comunicación durante la conversación SMTP con el proveedor de correo electrónico del destinatario. • BYOIPHostNameLookupUnavailable: Amazon SES no pudo buscar el nombre de anfitrión DNS para sus direcciones IP. Este tipo de retraso únicamente se produce cuando se utiliza Bring Your Own IP. • Undetermined: Amazon SES no pudo determinar el motivo del retraso en la entrega. • SendingDeferral: Amazon SES ha considera do apropiado aplazar de forma interna el mensaje.
`delayedRecipients`	Objeto que contiene información sobre el destinatario del correo electrónico.
`expirationTime`	La fecha y hora en que Amazon SES dejará de intentar entregar el mensaje. Este valor se muestra en formato ISO 8601.
`reportingMTA`	La dirección IP del Agente de transferencia de mensajes (MTA) que informó del retraso.
`timestamp`	Fecha y hora en que se produjo el retraso, que se muestra en formato ISO 8601.

Destinatarios con retraso

El objeto `delayedRecipients` contiene los siguientes valores.

Nombre del campo	Descripción
`emailAddress`	La dirección de correo electrónico que provocó el retraso en la entrega del mensaje.
`status`	El código de estado SMTP asociado al retraso de la entrega.
`diagnosticCode`	El código de diagnóstico proporcionado por el agente de transferencia de mensajes (MTA) receptor.

Objeto suscripción

El objeto JSON que contiene información acerca de un evento `Subscription` tiene los campos siguientes.

Nombre del campo	Descripción
`contactList`	El nombre de la lista de contacto está activado.
`timestamp`	La fecha y la hora, en formato ISO8601 (AAAA-MM-DDThh:mm:ss.sZ), cuando el ISP envió la notificación de suscripción.
`source`	La dirección de correo electrónico desde la que se envió el mensaje (la dirección MAIL FROM del sobre).
`newTopicPreferences`	Estructura de datos JSON (mapa) que especific a el estado de suscripción de todos los temas de la lista de contactos que indica el estado después de un cambio (contacto suscrito o cancelado).

Nombre del campo	Descripción
`oldTopicPreferences`	Estructura de datos JSON (mapa) que especifica el estado de suscripción de todos los temas de la lista de contactos que indica el estado antes del cambio (contacto suscrito o cancelado).

Preferencias de tema nuevo o antiguo

Los objetos `newTopicPreferences` y `oldTopicPreferences` contienen los siguientes valores.

Nombre del campo	Descripción
`unsubscribeAll`	Especifica si se canceló la suscripción del contacto de todos los temas de la lista de contactos.
`topicSubscriptionStatus`	Especifica el tema del campo `topicName` y asigna el estado de la suscripción (OptIn u OptOut) en el campo `subscriptionStatus` .
`topicDefaultSubscriptionStatus`	Especifica el tema del campo `topicName` y asigna el estado de la suscripción (OptIn u OptOut) en el campo `subscriptionStatus` .

Ejemplos de datos de eventos que Amazon SES publica en Amazon SNS

En esta sección se proporcionan ejemplos de los tipos de registros de evento de envío de correo electrónico que Amazon SES publica en Amazon SNS.

Temas de esta sección:

- Registro Bounce
- Registro Complaint

- Registro Delivery
- Registro Send
- Registro Reject
- Registro Open
- Registro Click
- Registro Rendering Failure
- DeliveryDelayregistro
- Registro de suscripción

> **Note**
>
> En los siguientes ejemplos en los que se utiliza un campo `tag`, se emplea la publicación de eventos a través de un conjunto de configuración para el que SES admite la publicación de etiquetas para todos los tipos de eventos. Si se utilizan las notificaciones de respuesta directamente en la identidad, SES no publica las etiquetas. Consulte cómo agregar etiquetas al crear un conjunto de configuración o modificar un conjunto de configuración.

Registro Bounce

El siguiente es el ejemplo de un registro de evento `Bounce` que Amazon SES publica en Amazon SNS.

```
{
  "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"
      ]
    }
  }
}
```

Registro Complaint

El siguiente es el ejemplo de un registro de evento `Complaint` que Amazon SES publica en Amazon SNS.

```
{
  "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"
      ]
    }
  }
}
```

Registro Delivery

El siguiente es el ejemplo de un registro de evento `Delivery` que Amazon SES publica en Amazon SNS.

```
{
  "eventType": "Delivery",
  "mail": {
    "timestamp": "2016-10-19T23:20:52.240Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination": [
      "recipient@example.com"
    ],
    "headersTruncated": false,
    "headers": [
      {
        "name": "From",
        "value": "sender@example.com"
      },
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
```

```
      },
      {
        "name": "Content-Type",
        "value": "text/html; charset=UTF-8"
      },
      {
        "name": "Content-Transfer-Encoding",
        "value": "7bit"
      }
    ],
    "commonHeaders": {
      "from": [
        "sender@example.com"
      ],
      "to": [
        "recipient@example.com"
      ],
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "subject": "Message sent from Amazon SES"
    },
    "tags": {
      "ses:configuration-set": [
        "ConfigSet"
      ],
      "ses:source-ip": [
        "192.0.2.0"
      ],
      "ses:from-domain": [
        "example.com"
      ],
      "ses:caller-identity": [
        "ses_user"
      ],
      "ses:outgoing-ip": [
        "192.0.2.0"
      ],
      "myCustomTag1": [
        "myCustomTagValue1"
      ],
      "myCustomTag2": [
        "myCustomTagValue2"
      ]
    }
  },
```

```
  "delivery": {
    "timestamp": "2016-10-19T23:21:04.133Z",
    "processingTimeMillis": 11893,
    "recipients": [
      "recipient@example.com"
    ],
    "smtpResponse": "250 2.6.0 Message received",
    "reportingMTA": "mta.example.com"
  }
}
```

Registro Send

El siguiente es el ejemplo de un registro de evento Send que Amazon SES publica en Amazon SNS. Algunos campos no siempre están presentes. Por ejemplo, con un correo electrónico con plantilla, el asunto se representa más tarde y se incluye en eventos posteriores.

```
{
  "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": {}
```

```
}
```

Registro Reject

El siguiente es el ejemplo de un registro de evento `Reject` que Amazon SES publica en Amazon SNS.

```
{
  "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"
  }
}
```

Registro Open

El siguiente es un ejemplo de un registro de evento Open que Amazon SES publica en Amazon SNS.

```
{
  "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"
  }
}
```

Registro Click

El siguiente es el ejemplo de un registro de evento `Click` que Amazon SES publica en Amazon SNS.

```
{
  "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"
  }
```

```
}
```

Registro Rendering Failure

El siguiente es el ejemplo de un registro de evento `Rendering Failure` que Amazon SES publica en Amazon SNS.

```
{
  "eventType":"Rendering Failure",
  "mail":{
    "timestamp":"2018-01-22T18:43:06.197Z",
    "source":"sender@example.com",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "tags":{
      "ses:configuration-set":[
        "ConfigSet"
      ]
    }
  },
  "failure":{
    "errorMessage":"Attribute 'attributeName' is not present in the rendering data.",
    "templateName":"MyTemplate"
  }
}
```

DeliveryDelayregistro

El siguiente es el ejemplo de un registro de evento `DeliveryDelay` que Amazon SES publica en Amazon SNS.

```
{
  "eventType": "DeliveryDelay",
  "mail":{
    "timestamp":"2020-06-16T00:15:40.641Z",
    "source":"sender@example.com",
    "sourceArn":"arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId":"123456789012",
```

```
    "messageId":"EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
    "destination":[
      "recipient@example.com"
    ],
    "headersTruncated":false,
    "tags":{
      "ses:configuration-set":[
        "ConfigSet"
      ]
    }
  },
  "deliveryDelay": {
    "timestamp": "2020-06-16T00:25:40.095Z",
    "delayType": "TransientCommunicationFailure",
    "expirationTime": "2020-06-16T00:25:40.914Z",
    "delayedRecipients": [{
      "emailAddress": "recipient@example.com",
      "status": "4.4.1",
      "diagnosticCode": "smtp; 421 4.4.1 Unable to connect to remote host"
    }]
  }
}
```

Registro de suscripción

El siguiente es un ejemplo de un registro de `Subscription` eventos que Amazon SES publica en Firehose.

```
{
  "eventType": "Subscription",
  "mail": {
    "timestamp": "2022-01-12T01:00:14.340Z",
    "source": "sender@example.com",
    "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
    "sendingAccountId": "123456789012",
    "messageId": "EXAMPLEe4bccb684-777bc8de-afa7-4970-92b0-f515137b1497-000000",
    "destination": ["recipient@example.com"],
    "headersTruncated": false,
    "headers": [
      {
        "name": "From",
        "value": "sender@example.com"
      },
```

```
      {
        "name": "To",
        "value": "recipient@example.com"
      },
      {
        "name": "Subject",
        "value": "Message sent from Amazon SES"
      },
      {
        "name": "MIME-Version",
        "value": "1.0"
      },
      {
        "name": "Content-Type",
        "value": "text/html; charset=UTF-8"
      },
      {
        "name": "Content-Transfer-Encoding",
        "value": "7bit"
      }
    ],
    "commonHeaders": {
      "from": ["sender@example.com"],
      "to": ["recipient@example.com"],
      "messageId": "EXAMPLEe4bccb684-777bc8de-afa7-4970-92b0-f515137b1497-000000",
      "subject": "Message sent from Amazon SES"
    },
    "tags": {
      "ses:operation": ["SendEmail"],
      "ses:configuration-set": ["ConfigSet"],
      "ses:source-ip": ["192.0.2.0"],
      "ses:from-domain": ["example.com"],
      "ses:caller-identity": ["ses_user"],
      "myCustomTag1": ["myCustomValue1"],
      "myCustomTag2": ["myCustomValue2"]
    }
  },
  "subscription": {
    "contactList": "ContactListName",
    "timestamp": "2022-01-12T01:00:17.910Z",
    "source": "UnsubscribeHeader",
    "newTopicPreferences": {
      "unsubscribeAll": true,
      "topicSubscriptionStatus": [
```

```
        {
          "topicName": "ExampleTopicName",
          "subscriptionStatus": "OptOut"
        }
      ]
    },
    "oldTopicPreferences": {
      "unsubscribeAll": false,
      "topicSubscriptionStatus": [
        {
          "topicName": "ExampleTopicName",
          "subscriptionStatus": "OptOut"
        }
      ]
    }
  }
}
```

Monitorear su reputación de remitente de Amazon SES

Amazon SES realiza un seguimiento activo de varias métricas que pueden dañar su reputación como remitente o que podrían provocar que sus tasas de envío de correo electrónico se reduzcan. Dos métricas importantes que tenemos en cuenta en este proceso son las tasas de rebotes y reclamaciones de su cuenta. Si la tasa de rebotes o de reclamaciones de su cuenta es demasiado alta, podríamos ponerla en proceso de revisión o suspender su capacidad para enviar correo electrónico.

Debido a que la tasa de rebotes y reclamos es tan importante para el estado de su cuenta, Amazon SES incluye una página de métricas de reputación en la consola de Amazon SES que puede utilizar para realizar un seguimiento de estas métricas. Las métricas de reputación también pueden mostrar información acerca de factores no relacionados con rebotes o reclamos que podrían dañar su reputación de remitente. Por ejemplo, si envía correo electrónico a una trampa de spam conocida, verá un mensaje en este panel.

Esta sección contiene información acerca de cómo acceder a las métricas de reputación, interpretar la información que contiene y configurar sistemas para que le notifiquen de forma activa los factores que podrían afectar a su reputación de remitente.

En esta sección, encontrará los temas siguientes:

- Uso de métricas de reputación para realizar un seguimiento de las tasas de rebotes y de reclamos
- Mensajes de métricas de reputación
- Creación de alarmas de monitoreo de reputación en CloudWatch
- Métricas de SNDS para direcciones IP dedicadas
- Suspensión automática del envío de correo electrónico

Uso de métricas de reputación para realizar un seguimiento de las tasas de rebotes y de reclamos

La página de la consola de métricas de reputación contiene la misma información que el equipo de Amazon SES ve al determinar el estado de las cuentas individuales.

Para ver las métricas de reputación

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación del lado izquierdo de la pantalla, elija Reputation metrics (Métricas de reputación).

   El panel muestra la siguiente información:

   - Account status (Estado de la cuenta): resumen del estado combinado de las tasas de rebotes y reclamos. Los valores posibles son:
     - Healthy: actualmente no hay ningún problema que afecte a su cuenta.
     - Under review (En proceso de revisión): su cuenta está en proceso de revisión. Si los problemas que han provocado que pongamos su cuenta en proceso de revisión no se resuelven antes de que finalice el periodo de revisión, podríamos suspender la capacidad de su cuenta para enviar correo electrónico.
     - Pending end of review decision (Pendiente de final de la decisión de revisión): su cuenta está en proceso de revisión. Debido a la naturaleza de los problemas que hicieron que pusiéramos su cuenta en proceso de revisión, tenemos que realizar una revisión manual de su cuenta antes de adoptar cualquier otra medida.
     - Sending paused (Envío suspendido): hemos suspendido la capacidad de su cuenta para enviar correo electrónico. Mientras que la capacidad de su cuenta para enviar correo electrónico esté suspendida, no podrá enviar correos electrónicos a través de Amazon SES. Puede solicitar que revisemos esta decisión. Para obtener más información sobre cómo solicitar una revisión, consulte Preguntas frecuentes acerca del proceso de revisión de envío de Amazon SES.
     - Pending sending pause (Pendiente de suspensión de envío): su cuenta está en proceso de revisión. Los problemas que han provocado que pongamos su cuenta en proceso de revisión no se han resuelto. En esta situación, normalmente suspendemos la capacidad de la cuenta para enviar correo. No obstante, dada la naturaleza de su cuenta, debemos revisarla antes de tomar alguna otra medida.
   - Bounce Rate: el porcentaje de correos electrónicos enviados desde su cuenta que han dado lugar a un rebote permanente. Consulte cómo se calcula su tasa de rebote.
   - Complaint Rate: el porcentaje de correos electrónicos enviados desde su cuenta que han dado lugar a que los destinatarios los notifiquen como spam. Consultar cómo se calcula su tasa de reclamos

> **Note**
>
> Las secciones Bounce Rate y Complaint Rate incluyen además mensajes de estado para sus métricas respectivas. A continuación, se muestra una lista de mensajes de estado que podrían mostrarse para estas métricas:
>
> - Healthy (Buen estado): la métrica está dentro de los niveles normales.
> - Almost healed (Casi recuperada): la métrica provocó que su cuenta se colocara en período de prueba. Desde que comenzó el periodo de revisión, la métrica ha estado por debajo de la tasa máxima. Si la métrica permanece por debajo de la tasa máxima, su estado cambiará a Healthy (En buen estado) antes de que finalice el periodo de revisión.
> - Under review (En proceso de revisión): la métrica provocó que su cuenta se colocara en proceso de revisión y sigue por encima de la tasa máxima. Si el problema que ha provocado que la métrica supere la tasa máxima no se resuelve antes de que finalice el periodo de revisión, podríamos suspender la capacidad de su cuenta para enviar correo electrónico.
> - Sending pause (Suspensión del envío): la métrica provocó que suspendiéramos la capacidad de su cuenta para enviar correo electrónico. Mientras esté suspendida la capacidad de su cuenta para enviar correo electrónico, no podrá enviar correo electrónico a través de Amazon SES. Puede solicitar que revisemos esta decisión. Para obtener más información sobre cómo enviar una solicitud de revisión, consulte Preguntas frecuentes acerca del proceso de revisión de envío de Amazon SES.
> - Pending sending pause (Pendiente de suspensión de envío): la métrica provocó que colocara su cuenta en proceso de revisión. Los problemas que han dado lugar a este periodo de revisión no se han resuelto. Estos problemas pueden hacer que suspendamos la capacidad de su cuenta para enviar correo electrónico. Un miembro del equipo de Amazon SES tiene que revisar su cuenta antes de que tomemos alguna medida adicional.

- Other Notifications (Otras notificaciones): si su cuenta está experimentando problemas relacionados con la reputación que no están relacionados con rebotes o reclamos, aquí se mostrará un mensaje breve. Para obtener más información sobre las notificaciones que se pueden mostrar en esta área, consulte Mensajes de métricas de reputación.

Mensajes de métricas de reputación

La página de la consola de métricas de reputación de Amazon SES ofrece métricas importantes relacionadas con su cuenta. En las siguientes secciones, se describen los mensajes que podrían aparecer en este panel y se ofrecen consejos e información que podría utilizar para resolver los problemas relacionados con la reputación del remitente.

Esta sección contiene información acerca de los siguientes tipos de notificaciones:

- Mensajes de estado
- Notificación de tasa de rebotes
- Notificación de tasa de reclamaciones
- Notificación de organización antispam
- Notificación de bombardeo de lista
- Notificaciones de retroalimentación directa
- Notificación de lista de bloqueo de dominios
- Notificación de revisión interna
- Notificación de proveedor de bandeja de correo
- Notificaciones de retroalimentación de destinatario
- Notificación de cuenta relacionada
- Notificación de trampa de spam
- Notificación de sitio vulnerable
- Notificación de credenciales comprometidas
- Otras notificaciones

Mensajes de estado

Cuando utilice la página de la consola de métricas de reputación, verá un mensaje que describe el estado de su cuenta de Amazon SES. A continuación se muestra una lista de posibles valores de estado de la cuenta:

- Healthy: actualmente no hay ningún problema que afecte a su cuenta.
- Under review (En proceso de revisión): su cuenta está en proceso de revisión. Si los problemas que han provocado que pongamos su cuenta en proceso de revisión no se resuelven antes de que

finalice el periodo de revisión, podríamos suspender la capacidad de su cuenta para enviar correo electrónico.

- Pending end of review decision (Pendiente de final de la decisión de revisión): su cuenta está en proceso de revisión. Debido a la naturaleza de los problemas que hicieron que pusiéramos su cuenta en proceso de revisión, tenemos que realizar una revisión manual de su cuenta antes de adoptar cualquier otra medida.
- Sending paused (Envío suspendido): hemos suspendido la capacidad de su cuenta para enviar correo electrónico. Mientras que la capacidad de su cuenta para enviar correo electrónico esté suspendida, no podrá enviar correos electrónicos a través de Amazon SES. Puede solicitar que revisemos esta decisión. Para obtener más información sobre cómo solicitar una revisión, consulte Preguntas frecuentes acerca del proceso de revisión de envío de Amazon SES.
- Pending sending pause (Pendiente de suspensión de envío): su cuenta está en proceso de revisión. Los problemas que han provocado que pongamos su cuenta en proceso de revisión no se han resuelto. En esta situación, normalmente suspendemos la capacidad de la cuenta para enviar correo. No obstante, dada la naturaleza de su cuenta, debemos revisarla antes de tomar alguna otra medida.

Además, las secciones Bounce Rate (Tasa de rebotes) y Complaint Rate (Tasa de reclamos) de la página de métricas de reputación muestra los resúmenes de estado de sus métricas respectivas. A continuación se muestra una lista de posibles valores de estado de la métrica:

- Healthy (Buen estado): la métrica está dentro de los niveles normales.
- Almost healed (Casi recuperada): la métrica provocó que su cuenta se colocara en período de prueba. Desde que comenzó el periodo de revisión, la métrica ha estado por debajo de la tasa máxima. Si la métrica permanece por debajo de la tasa máxima, su estado cambiará a Healthy (En buen estado) antes de que finalice el periodo de revisión.
- Under review (En proceso de revisión): la métrica provocó que su cuenta se colocara en proceso de revisión y sigue por encima de la tasa máxima. Si el problema que ha provocado que la métrica supere la tasa máxima no se resuelve antes de que finalice el periodo de revisión, podríamos suspender la capacidad de su cuenta para enviar correo electrónico.
- Sending pause (Suspensión del envío): la métrica provocó que suspendiéramos la capacidad de su cuenta para enviar correo electrónico. Mientras esté suspendida la capacidad de su cuenta para enviar correo electrónico, no podrá enviar correo electrónico a través de Amazon SES. Puede solicitar que revisemos esta decisión. Para obtener más información sobre cómo enviar una

solicitud de revisión, consulte Preguntas frecuentes acerca del proceso de revisión de envío de Amazon SES.

- Pending sending pause (Pendiente de suspensión de envío): la métrica provocó que colocara su cuenta en proceso de revisión. Los problemas que han dado lugar a este periodo de revisión no se han resuelto. Estos problemas pueden hacer que suspendamos la capacidad de su cuenta para enviar correo electrónico. Un miembro del equipo de Amazon SES tiene que revisar su cuenta antes de que tomemos alguna medida adicional.

Notificación de tasa de rebotes

Esta sección contiene información adicional acerca de las notificaciones de tasa de rebotes mostradas en la página de métricas de reputación de Amazon SES.

¿Por qué ha recibido esta notificación?

Ha recibido esta notificación porque el porcentaje de rebote de su cuenta es demasiado alto. La tasa de rebotes se basa en el número de rechazos permanentes generados por su cuenta de Amazon SES. Los proveedores de correo electrónico interpretan una tasa elevada de rebotes como una señal de que el remitente no está administrando correctamente su lista de destinatarios y de que podría estar enviando correo electrónico no solicitado.

Un rebote permanente se produce cuando se envía un correo electrónico a una dirección que no existe. Amazon SES no tiene en cuenta los rebotes temporales (que se producen cuando la dirección de un destinatario no puede recibir mensajes temporalmente) en este cálculo. Los correos electrónicos rebotados que envíe a direcciones y dominios verificados, así como los enviados al simulador de bandeja de correo de Amazon SES, tampoco se tienen en cuenta en este cálculo.

La tasa de rebote se calcula en función de un volumen representativo de correo electrónico. Se considera como volumen representativo una cantidad de correo electrónico que representa sus prácticas de envío típicas. Para ser justos con los remitentes de volúmenes grandes y pequeños, el volumen representativo es distinto para cada cuenta y cambia a medida que cambian los patrones de envío de la cuenta.

Para obtener los mejores resultados, mantenga una tasa de rebote por debajo del 5 %. Las tasas de rebotes más altas pueden afectar a la entrega de sus correos electrónicos. Si la tasa de rebote es del 5 % o superior, revisaremos su cuenta de forma automática. Si la tasa de rebote es del 10 % o superior, es posible que pausemos la opción de enviar correos electrónicos desde su cuenta hasta que resuelva el problema que ha provocado esta tasa de rebote tan elevada.

Qué puede hacer para resolver el problema

Si aún no lo ha hecho, implemente un proceso para capturar y administrar rebotes y quejas. Es obligatorio que todas las cuentas de Amazon SES implementen estos procesos. Para obtener más información, consulte Métricas de éxito para los programas de correo electrónico.

A continuación, determine qué direcciones de correo electrónico presentan rebotes y cree e implemente un plan para reducir o eliminar dichos rebotes. Si la capacidad de su cuenta para enviar correo electrónico ya está en pausa, inicie sesión en la AWS Management Console y vaya a AWS Support. Responda al caso que abrimos en su nombre.

Si su cuenta está en proceso de revisión

Si la tasa de rebotes de su cuenta sigue estando por encima del 10 % al finalizar el periodo de revisión, podríamos suspender la capacidad de su cuenta para enviar correo electrónico hasta que resuelva el problema.

Si ha implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. En su respuesta al caso, describa los cambios que implementó. Si estamos de acuerdo en que los cambios reducirán su tasa de rebotes, ajustamos nuestros cálculos para tener en cuenta solo los rebotes recibidos después de haber implementado sus cambios.

Si se ha suspendido la capacidad de su cuenta para enviar correo electrónico

Puede solicitar que reconsideremos esta decisión. Para obtener más información, consulte Preguntas frecuentes acerca del proceso de revisión de envío de Amazon SES.

Cuando implemente los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. Incluya detalles de las medidas que ha tomado para resolver este problema, así como detalles de sus planes para garantizar que este problema no se vuelva a producir. Una vez que recibamos su solicitud, revisaremos la información que ha proporcionado y cambiaremos el estado de su cuenta, si es necesario.

Notificación de tasa de reclamaciones

Esta sección contiene información adicional acerca de las notificaciones de tasa de reclamos mostradas en la página de métricas de reputación de Amazon SES.

¿Por qué ha recibido esta notificación?

Ha recibido esta notificación porque la tasa de quejas de su cuenta es demasiado alta. La tasa de reclamos se basa en el número de reclamos generados por su cuenta de Amazon SES. Los proveedores de correo electrónico interpretan una tasa elevada de quejas como una señal de que el remitente no está administrando correctamente su lista de destinatarios y de que podría estar enviando correo electrónico no solicitado.

Una queja se produce cuando un destinatario identifica un correo electrónico que usted ha enviado como spam. Esto suele ocurrir cuando el destinatario utiliza el botón Report Spam (Marcar como spam) en su cliente de correo electrónico. Los reclamos generados por los correos electrónicos que envía al simulador de bandeja de correo de Amazon SES no se tienen en cuenta en este cálculo.

La tasa de reclamos se calcula en función de un volumen representativo de correo electrónico. Se considera como volumen representativo una cantidad de correo electrónico que representa sus prácticas de envío típicas. Para ser justos con los remitentes de volúmenes grandes y pequeños, el volumen representativo es distinto para cada cuenta y cambia a medida que cambian los patrones de envío de la cuenta.

Para obtener los mejores resultados, mantenga una tasa de quejas por debajo del 0,1 %. Las tasas de reclamos más altas pueden afectar a la entrega de sus correos electrónicos. Si la tasa de quejas es del 0,1 % o superior, revisaremos su cuenta de forma automática. Si la tasa de quejas es del 0,5 % o superior, es posible que pausemos la opción de enviar correos electrónicos desde su cuenta hasta que resuelva el problema que ha provocado esta tasa de quejas tan elevada.

Qué puede hacer para resolver el problema

Si aún no lo ha hecho, implemente un proceso para capturar y administrar rebotes y quejas. Es obligatorio que todas las cuentas de Amazon SES implementen estos procesos. Para obtener más información, consulte Métricas de éxito para los programas de correo electrónico.

A continuación, determine cuáles de los mensajes que envía dan lugar a reclamaciones e implemente un plan para reducir estas reclamaciones. Si la capacidad de su cuenta para enviar correo electrónico ya está suspendida, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre

Aunque debe dejar de enviar de inmediato a aquellas direcciones que hayan presentado reclamaciones, es importante que identifique los factores que hacen que los destinatarios reclamen. Después de identificar estos factores, ajuste su comportamiento de envío de correo electrónico para corregirlo.

Si su cuenta está en proceso de revisión

Si la tasa de reclamaciones de su cuenta sigue estando por encima del 0,5 % al finalizar el periodo de revisión, podríamos suspender la capacidad de su cuenta para enviar correo electrónico hasta que resuelva el problema.

Si ha implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. En su respuesta al caso, describa los cambios que implementó. Si estamos de acuerdo en que los cambios reducirán su tasa de quejas, ajustaremos nuestros cálculos para tener en cuenta solo las quejas que se hayan recibido después de haber implementado los cambios.

Si se ha suspendido la capacidad de su cuenta para enviar correo electrónico

Puede solicitar que reconsideremos esta decisión. Para obtener más información, consulte Preguntas frecuentes acerca del proceso de revisión de envío de Amazon SES.

Cuando haya implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. Incluya detalles de las medidas que ha tomado para resolver este problema, así como detalles de sus planes para garantizar que este problema no se vuelva a producir. Una vez que recibamos su solicitud, revisaremos la información que ha proporcionado y cambiaremos el estado de su cuenta, si es necesario.

Notificación de organización antispam

Esta sección contiene información adicional acerca de las notificaciones de organización antispam mostradas en la página de métricas de reputación de Amazon SES.

¿Por qué ha recibido esta notificación?

Una organización antispam reconocida ha informado de que sus sistemas han marcado parte de los contenidos que se envían desde su cuenta de Amazon SES como correo no solicitado o problemático.

No podemos proporcionar información sobre los mensajes específicos que han provocado que la organización antispam marque su contenido como problemático. No podemos facilitarle el nombre de la organización que generó el informe. Normalmente, las organizaciones antispam tienen en cuenta una combinación de los siguientes factores: retroalimentación del destinatario, métricas de

implicación de mensajes, intentos de entrega a direcciones no válidas, contenido marcado por los filtros de spam e incidencias de trampas de spam. Esto no es una lista exhaustiva; otros factores podrían hacer que estas organizaciones marquen el contenido.

Qué puede hacer para resolver el problema

Para solucionar este problema, debe determinar qué aspectos de su programa de envío de correo electrónico podrían ocasionar que la organización antispam marque su correo electrónico como problemático. Tiene que cambiar su programa de envío para resolver estos problemas.

Si su cuenta está en proceso de revisión

Al finalizar el periodo de revisión, si la organización antispam sigue identificando el correo electrónico enviado desde su cuenta como problemático, podríamos suspender la capacidad de su cuenta para enviar correo electrónico hasta que resuelva el problema.

Si ha implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. En su mensaje, proporcione detalles de los cambios que ha realizado. Cuando recibamos esta información, ampliaremos el período de revisión para garantizar que solo analizamos las notificaciones de la organización antispam que hemos recibido después de que haya implementado los cambios. Si, al finalizar este periodo de revisión ampliado, su cuenta ya no está en la lista de la organización antispam, eliminaremos el periodo de revisión de su cuenta.

Si se ha suspendido la capacidad de su cuenta para enviar correo electrónico

Puede solicitar que reconsideremos esta decisión. Para obtener más información, consulte Preguntas frecuentes acerca del proceso de revisión de envío de Amazon SES.

Cuando haya implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. Incluya detalles de las medidas que ha tomado para resolver este problema, así como detalles de sus planes para garantizar que este problema no se vuelva a producir. Una vez que recibamos su solicitud, revisaremos la información que ha proporcionado y cambiaremos el estado de su cuenta, si es necesario.

Notificación de bombardeo de lista

Esta sección contiene información adicional acerca de las notificaciones de bombardeo de lista mostradas en la página de métricas de reputación de Amazon SES.

¿Por qué ha recibido esta notificación?

Una organización antispam ha identificado que sus procesos de envío de correo electrónico son vulnerables al "bombardeo de lista". El bombardeo de lista es una forma de abuso en la que un atacante registra un gran número de direcciones de correo electrónico en un formulario basado en la web. El bombardeo de lista puede provocar interrupciones del servicio para los usuarios de servicios de correo electrónico afectados. También puede provocar que los proveedores de correo electrónico bloqueen el correo electrónico.

Las organizaciones antispam utilizan métodos patentados para identificar sitios vulnerables al bombardeo de lista. Por este motivo, no podemos proporcionar detalles adicionales sobre el problema que llevó a la organización antispam a identificar el proceso de envío de correo electrónico como problemático. No podemos compartir el nombre de la organización que identificó el problema.

Qué puede hacer para resolver el problema

Debe examinar todos los formularios de registro basados en la web para asegurarse de que no son vulnerables a este tipo de abuso. Cada formulario debe incluir un CAPTCHA para evitar que los scripts automatizados envíen solicitudes de suscripción. Además, cuando nuevos usuarios se registren para su producto o servicio, envíeles un correo electrónico para confirmar si realmente tienen la intención de registrarse. No envíe ningún correo electrónico adicional a los clientes a menos que se inscriban explícitamente para recibir sus comunicaciones.

Por último, debe realizar un "pase de permiso" en la lista de correo electrónico. En un pase de permiso, envía un correo electrónico a todos los clientes preguntándoles si aún quieren recibir sus correos electrónicos. Envíe correos electrónicos solo a los clientes que verifiquen que desean seguir recibiéndolos.

Si su cuenta está en proceso de revisión

Al finalizar el periodo de revisión, si la organización antispam sigue identificando el correo electrónico enviado desde su cuenta como problemático, podríamos suspender la capacidad de su cuenta para enviar correo electrónico hasta que resuelva el problema.

Si ha implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. En su mensaje, proporcione detalles de los cambios que ha realizado. Cuando recibamos esta información, ampliaremos el período de revisión para garantizar que solo analizamos las notificaciones de la organización antispam que hemos recibido después de que haya implementado los cambios. Si,

al finalizar este periodo de revisión ampliado, su cuenta ya no está en la lista de la organización antispam, eliminaremos el periodo de revisión de su cuenta.

Si se ha suspendido la capacidad de su cuenta para enviar correo electrónico

Puede solicitar que reconsideremos esta decisión. Para obtener más información, consulte Preguntas frecuentes acerca del proceso de revisión de envío de Amazon SES.

Cuando haya implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. Incluya detalles de las medidas que ha tomado para resolver este problema, así como detalles de sus planes para garantizar que este problema no se vuelva a producir. Una vez que recibamos su solicitud, revisaremos la información que ha proporcionado y cambiaremos el estado de su cuenta, si es necesario.

Notificaciones de retroalimentación directa

Esta sección contiene información adicional acerca de las notificaciones de retroalimentación directa mostradas en la página de métricas de reputación de Amazon SES.

¿Por qué ha recibido esta notificación?

Un número importante de usuarios ha contactado con Amazon SES directamente para informar de mensajes que han recibido de una dirección o un dominio asociados a su cuenta de Amazon SES. Este tipo de retroalimentación no es visible en los reclamos notificados directamente por los proveedores de bandeja de correo y no se incluye en las métricas de rebotes y reclamos que se muestran en la página de métricas de reputación.

Para proteger la privacidad de los usuarios que han notificado estos problemas, no podemos proporcionar sus direcciones de correo electrónico.

Los destinatarios pueden reclamar a Amazon SES cuando reciben mensajes a los que no se han suscrito, cuando no reciben el tipo de correo que esperaban recibir, cuando no encuentran útil o interesante el correo electrónico que reciben, cuando no reconocen que se registraron para recibir los mensajes o cuando reciben demasiados mensajes. Esta lista no es exhaustiva; los factores relevantes en su caso dependen de su programa de envío de correo electrónico específico.

Qué puede hacer para resolver el problema

Le recomendamos que implemente una doble estrategia de confirmación, tal y como se describe en Creación y mantenimiento de sus listas, para adquirir nuevas direcciones y que solo envíe correos electrónicos a aquellas direcciones que hayan completado el proceso de confirmación doble.

Además, debe eliminar de sus listas aquellas direcciones que no hayan interactuado con sus correos electrónicos recientemente. Puede utilizar el seguimiento de mensajes abiertos y en los que se ha hecho clic, tal como se describe en Monitoreo de la actividad de envío de Amazon SES, para determinar qué usuarios están visualizando e interactuando con el contenido que envía.

Si su cuenta está en proceso de revisión

Al finalizar el periodo de revisión, si Amazon SES sigue recibiendo un número importante de reclamos directos acerca de los mensajes enviados desde su cuenta, podríamos suspender la capacidad de su cuenta para enviar correo electrónico hasta que resuelva el problema.

Si ha implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. Proporcione información detallada sobre las medidas que ha tomado para resolver el problema y explique de qué manera estos pasos evitarán que el problema vuelva a producirse en el futuro. Si estamos de acuerdo en que los cambios que ha realizado solucionan el problema de forma adecuada, cancelaremos el período de revisión de su cuenta.

Si se ha suspendido la capacidad de su cuenta para enviar correo electrónico

Puede solicitar que reconsideremos esta decisión. Para obtener más información, consulte Preguntas frecuentes acerca del proceso de revisión de envío de Amazon SES.

Cuando haya implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. Incluya detalles de las medidas que ha tomado para resolver este problema, así como detalles de sus planes para garantizar que este problema no se vuelva a producir. Una vez que recibamos su solicitud, revisaremos la información que ha proporcionado y cambiaremos el estado de su cuenta, si es necesario.

Notificación de lista de bloqueo de dominios

Esta sección contiene información adicional acerca de las notificaciones de lista de bloqueo de dominios mostradas en la página de métricas de reputación de Amazon SES.

¿Por qué ha recibido esta notificación?

Los correos electrónicos enviados desde su cuenta de Amazon SES contienen referencias a dominios que se han incluido en una lista de bloqueo de dominios acreditada. Los dominios de estas listas suelen estar asociados a comportamientos abusivos o malintencionados. Los dominios en cuestión podrían estar o no en los dominios desde los que envía correo electrónico. Los mensajes que incluyan referencias o enlaces a un dominio incluido en una lista de bloqueo o que incluyan imágenes alojadas en dicho dominio, también podrían marcarse.

No podemos proporcionar los nombres de los dominios que hacen que los mensajes aparezcan marcados ni identificar qué correos electrónicos se han marcado de esta forma.

Qué puede hacer para resolver el problema

En primer lugar, cree una lista de todos los dominios a los que se hace referencia en los mensajes de correo electrónico que envíe a través de Amazon SES. A continuación, utilice la herramienta Domain Lookup Tool de Spamhaus para determinar los dominios de su correo electrónico que están en la lista de bloqueo de dominios. Es posible que en esta lista de bloqueo haya más de un dominio al que se haga referencia en los correos electrónicos que envía.

La lista de bloqueo de dominios de Spamhaus no está afiliada a Amazon SES ni a AWS. No garantizamos la exactitud de los dominios que aparecen en ella. La lista de bloqueo de dominios de Spamhaus y la herramienta Domain Lookup Tool son propiedad de Spamhaus Project, que es responsable de su funcionamiento y mantenimiento.

Si su cuenta está en proceso de revisión

Buscamos referencias a los dominios que se han utilizado con fines maliciosos en los correos electrónicos que envía durante el período de revisión. Si los correos electrónicos aún contienen un número significativo de referencias a dichos dominios, podríamos suspender la capacidad de su cuenta para enviar correo electrónico hasta que resuelva el problema.

Si ha implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. En su mensaje, proporcione detalles de los cambios que ha realizado. Cuando recibamos esta información, ampliaremos el período de revisión para garantizar que solo analizamos el número de dominios bloqueados presentes en su correo electrónico después de que haya implementado los cambios. Al finalizar este período de revisión ampliado, si el número de notificaciones de lista de bloqueo de dominios se ha reducido o no hay ninguna y creemos que ha adoptado medidas para evitar que este problema se repita en el futuro, procederemos a cancelar el período de revisión de su cuenta.

Si se ha suspendido la capacidad de su cuenta para enviar correo electrónico

Puede solicitar que reconsideremos esta decisión. Para obtener más información, consulte Preguntas frecuentes acerca del proceso de revisión de envío de Amazon SES.

Cuando haya implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. Incluya detalles de las medidas que ha tomado para resolver este problema, así como detalles de sus planes para garantizar que este problema no se vuelva a producir. Una vez que recibamos su solicitud, revisaremos la información que ha proporcionado y cambiaremos el estado de su cuenta, si es necesario.

Notificación de revisión interna

Esta sección contiene información adicional acerca de las notificaciones de revisión interna mostradas en la página de métricas de reputación de Amazon SES.

¿Por qué ha recibido esta notificación?

Una revisión exhaustiva de su cuenta identificó diversas características que pueden provocar que los proveedores de buzones de correo o los destinatarios identifiquen sus mensajes como spam.

Para proteger nuestro proceso de detección de abusos, no podemos revelar los factores específicos que han llevado a marcar a su cuenta de este modo.

Los factores habituales que pueden dar lugar a esta determinación son, entre otros, los siguientes:

- Mensajes marcados por los sistemas antispam comerciales.
- Contenido de mensaje que implica que el destinatario no ha solicitado explícitamente el correo electrónico.
- Discrepancias entre el remitente del mensaje y la marca que aparece en el cuerpo del correo electrónico.
- Contenido que no aclara quién es el remitente.
- Envío de mensajes que tratan con contenido asociado con correo electrónico no solicitado.
- Patrones de formato asociados a correo electrónico no solicitado.
- Envío desde dominios con mala reputación o hacer referencia a los mismos.

Esta no es una lista completa. Los motivos concretos de esta notificación podrían ser una combinación de cualquiera de estos factores o bien algún motivo no incluido en la lista.

Qué puede hacer para resolver el problema

Las siguientes sugerencias podrían ayudar a reducir la gravedad del problema:

- Asegúrese de que los únicos destinatarios con quienes se pone en contacto sean aquellos que hayan solicitado de forma explícita recibir sus correos electrónicos.
- No compre, alquile o tome prestadas listas de destinatarios de correo electrónico nunca.
- No intente ocultar su identidad o el propósito de la comunicación en los mensajes que envía.
- Cree una lista de todos los dominios a los que se hace referencia en los mensajes de correo electrónico que envía a través de Amazon SES y utilice la herramienta Spamhaus Domain Lookup de https://www.spamhaus.org/lookup/ para determinar si alguno de estos dominios aparece en la lista de bloqueo de dominios de Spamhaus.
- No olvide seguir las prácticas recomendadas del sector a la hora de diseñar sus mensajes de correo electrónico.

Esta lista no es exhaustiva, pero debería ayudarle a identificar algunos de los factores más comunes que podrían dar lugar a que su correo electrónico se marque.

La lista de bloqueo de dominios de Spamhaus no está afiliada a Amazon SES ni a AWS. No garantizamos la exactitud de los dominios que aparecen en ella. La lista de bloqueo de dominios de Spamhaus y la herramienta Domain Lookup Tool son propiedad de Spamhaus Project, que es responsable de su funcionamiento y mantenimiento.

Si su cuenta está en proceso de revisión o se ha suspendido su capacidad para enviar correo electrónico

Cuando haya implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. Proporcione información detallada sobre las medidas que ha tomado para resolver el problema y explique de qué manera estos pasos evitarán que el problema vuelva a producirse en el futuro. Si estamos de acuerdo en que los cambios que ha realizado solucionan el problema de forma adecuada, cancelaremos el período de revisión o eliminaremos la suspensión del envío desde su cuenta.

Si eliminamos el periodo de revisión o la suspensión del envío desde su cuenta y observamos el mismo problema en otro momento, podríamos poner su cuenta en proceso de revisión o suspender su capacidad para enviar correo electrónico de nuevo. En casos extremos, o si observamos el mismo problema repetidamente, podríamos suspender de forma permanente la capacidad de su cuenta para enviar correo electrónico.

Consulte Preguntas frecuentes acerca del proceso de revisión de envío de Amazon SES para obtener más información sobre qué hacer si su cuenta está en proceso de revisión o se ha suspendido su capacidad para enviar correo electrónico.

Notificación de proveedor de bandeja de correo

Esta sección contiene información adicional acerca de las notificaciones de proveedor de bandeja de correo mostradas en la página de métricas de reputación de Amazon SES.

¿Por qué ha recibido esta notificación?

Un destacado proveedor de bandeja de correo nos ha informado que se está enviando correo no solicitado o malintencionado desde una dirección o un dominio asociado con su cuenta de Amazon SES.

No podemos compartir la identidad de la organización que generó este informe. Además, no tenemos información sobre los factores específicos que han provocado que el proveedor de bandeja de correo emita el informe. Normalmente, los proveedores de bandeja de correo toman este tipo de determinación a partir de retroalimentación de los clientes, métricas de compromiso de clientes, intentos de entregas a direcciones no válidas y contenido marcado por filtros de spam. Esta lista no es exhaustiva; es posible que haya otros factores que hayan provocado que el proveedor de bandeja de correo marque su contenido.

Qué puede hacer para resolver el problema

Para solucionar este problema, debe determinar qué aspectos de su programa de envío de correo electrónico podrían haber provocado que los proveedores de bandeja de correo marquen su correo como problemático. Seguidamente debe cambiar su programa de envío para resolver estos problemas.

Si su cuenta está en proceso de revisión

Al finalizar el periodo de revisión, si el proveedor de bandeja de correo sigue identificando el correo proveniente de su cuenta como problemático, podríamos detener la capacidad de su cuenta para enviar correo electrónico hasta que resuelva el problema.

Si ha implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. En su mensaje, proporcione detalles de los cambios que ha realizado. Cuando recibamos esta información, ampliaremos el período de revisión para garantizar que solo analizamos el número de notificaciones de proveedor de bandeja de correo que recibimos después de implementar los cambios. Al finalizar este periodo de revisión ampliado, si el proveedor de bandeja de correo deja de notificar su cuenta como problemática, podríamos eliminar la revisión de su cuenta.

Si se ha suspendido la capacidad de su cuenta para enviar correo electrónico

Puede solicitar que reconsideremos esta decisión. Para obtener más información, consulte Preguntas frecuentes acerca del proceso de revisión de envío de Amazon SES.

Cuando haya implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. Incluya detalles de las medidas que ha tomado para resolver este problema, así como detalles de sus planes para garantizar que este problema no se vuelva a producir. Una vez que recibamos su solicitud, revisaremos la información que ha proporcionado y cambiaremos el estado de su cuenta, si es necesario.

Notificaciones de retroalimentación de destinatario

Esta sección contiene información adicional acerca de las notificaciones de retroalimentación de destinatario mostradas en la página de métricas de reputación de Amazon SES.

¿Por qué ha recibido esta notificación?

Un importante proveedor de bandeja de correo nos ha informado de que un gran número de sus usuarios están notificando correo no solicitado enviado desde su cuenta de Amazon SES. Este tipo de retroalimentación no es visible en los reclamos notificados por los proveedores de bandeja de correo directamente y no se incluye en las notificaciones de rebote y reclamo de Amazon SES.

Un gran número de reclamos puede tener un impacto negativo en todos los usuarios de Amazon SES. Para proteger su reputación y la de otros clientes de Amazon SES, tomamos medidas de inmediato cuando una cuenta recibe un determinado número de reclamos.

No podemos proporcionar una lista de direcciones de correo electrónico específicas que notifiquen su correo electrónico no solicitado. Además, no podemos compartir el nombre del proveedor de bandeja de correo que nos ha informado de este problema.

Qué puede hacer para resolver el problema

Para solucionar este problema, debe determinar qué aspectos de su programa de envío de correo electrónico podrían estar causando que los destinatarios formulen reclamaciones contra los mensajes de correo electrónico que reciben de usted. Después de identificar estos factores, cambie sus prácticas de envío de correo electrónico para corregirlo.

Para conseguir nuevas direcciones, le recomendamos que implemente una doble estrategia de confirmación, tal y como se describe en las direcciones Creación y mantenimiento de sus listas. Le recomendamos que solo envíe correo electrónico a aquellas direcciones que hayan completado un proceso de confirmación doble.

Además, debe eliminar de sus listas aquellas direcciones que no hayan interactuado con sus correos electrónicos recientemente. Puede utilizar el seguimiento de mensajes abiertos y en los que se ha hecho clic, tal como se describe en Monitoreo de la actividad de envío de Amazon SES, para determinar qué usuarios están visualizando e interactuando con el contenido que envía.

Si su cuenta está en proceso de revisión

Al finalizar el periodo de revisión, si el proveedor de bandeja de correo sigue notificando un número de reclamaciones importante, podríamos detener la capacidad de su cuenta para enviar correo electrónico hasta que resuelva el problema.

Si ha implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. En su mensaje, proporcione detalles de los cambios que ha realizado. Cuando recibamos esta información, ampliaremos el período de revisión para garantizar que solo analizamos el número de quejas de proveedor de bandeja de correo que recibimos después de implementar los cambios. Al finalizar este periodo de revisión ampliado, si el número de reclamaciones de proveedor de correo se ha reducido o eliminado, podríamos eliminar la revisión de su cuenta.

Si se ha suspendido la capacidad de su cuenta para enviar correo electrónico

Puede solicitar que reconsideremos esta decisión. Para obtener más información, consulte Preguntas frecuentes acerca del proceso de revisión de envío de Amazon SES.

Cuando haya implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. Incluya detalles de las medidas que ha tomado para resolver este problema, así como detalles de sus planes para garantizar que este problema no se vuelva a producir. Una vez que recibamos su solicitud, revisaremos la información que ha proporcionado y cambiaremos el estado de su cuenta, si es necesario.

Notificación de cuenta relacionada

Esta sección contiene información adicional acerca de las notificaciones de cuenta relacionadas mostradas en la página de métricas de reputación de Amazon SES.

¿Por qué ha recibido esta notificación?

Hemos detectado graves problemas relacionados con los correos electrónicos que se envían desde otra cuenta de Amazon SES. Creemos que la cuenta problemática está relacionada con su cuenta de Cuenta de AWS, por lo que hemos adoptado medidas para evitar problemas similares.

Qué puede hacer para resolver el problema

Cuando detenemos la capacidad de enviar correo electrónico de una cuenta, siempre enviamos información sobre los motivos de esta decisión al propietario de esa cuenta. Consulte el correo electrónico que le enviamos al propietario de la cuenta relacionada para obtener más información.

En primer lugar, debería solucionar los problemas en la cuenta relacionada. Cuando haya implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. Proporcione información detallada sobre las medidas que ha tomado para resolver el problema y explique de qué manera estos pasos evitarán que el problema vuelva a producirse en el futuro. Si estamos de acuerdo en que los cambios que ha realizado solucionan el problema de forma adecuada, cancelaremos el período de revisión o eliminaremos la suspensión del envío desde su cuenta.

Notificación de trampa de spam

Esta sección contiene información adicional acerca de las notificaciones de trampa de spam mostradas en la página de métricas de reputación de Amazon SES.

¿Por qué ha recibido esta notificación?

Una organización antispam de terceros nos ha informado de que sus direcciones de trampa de spam han recibido recientemente correo electrónico de direcciones o dominios verificados asociados a su cuenta de Amazon SES.

Una trampa de spam es una dirección de correo electrónico inactiva que se utiliza exclusivamente para atraer correo electrónico no solicitado (spam). Un gran número de informes de trampa de spam puede tener un impacto negativo en todos los usuarios de Amazon SES. Para proteger su reputación y la de otros clientes de Amazon SES, tomamos medidas de inmediato cuando una cuenta envía un volumen determinado de correo electrónico en direcciones de trampa de spam.

Qué puede hacer para resolver el problema

No podemos revelar las direcciones de correo electrónico asociadas con la trampa de spam que ha encontrado. Estas direcciones son vigiladas estrechamente por las organizaciones que las poseen y, una vez que las direcciones son conocidas, dejan de ser útiles.

El envío de correo electrónico a direcciones de trampa de spam indica que hay un problema con la forma en que adquiere las direcciones de correo electrónico de sus clientes. Por ejemplo, las listas de direcciones de correo electrónico compradas pueden contener direcciones de trampa de spam, por lo que el envío a las listas adquiridas o alquiladas está prohibido por los términos de servicio de Amazon SES. Para conseguir nuevas direcciones, le recomendamos que implemente una doble estrategia de confirmación, tal y como se describe en las direcciones Creación y mantenimiento de sus listas. Le recomendamos que solo envíe correo electrónico a aquellas direcciones que hayan completado un proceso de confirmación doble.

Además, debe eliminar de sus listas aquellas direcciones que no hayan interactuado con sus correos electrónicos recientemente. Puede utilizar el seguimiento de mensajes abiertos y en los que se ha hecho clic, tal como se describe en Monitoreo de la actividad de envío de Amazon SES, para determinar qué usuarios están visualizando e interactuando con el contenido que envía.

Si su cuenta está en proceso de revisión

Al finalizar el periodo de revisión, si se siguen enviando mensajes a las direcciones de trampa de spam desde su cuenta, podríamos detener la capacidad de esta para enviar correo electrónico hasta que resuelva el problema.

Si ha implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. En su mensaje, proporcione detalles de los cambios que ha realizado. Cuando recibamos esta información, ampliaremos el período de revisión para garantizar que solo analizamos el número de informes de trampa de spam que recibimos después de implementar los cambios. Al finalizar este periodo de revisión ampliado, si el número de informes de trampa de spam se ha reducido o eliminado, podríamos eliminar la revisión de su cuenta.

Si se ha suspendido la capacidad de su cuenta para enviar correo electrónico

Puede solicitar que reconsideremos esta decisión. Para obtener más información, consulte Preguntas frecuentes acerca del proceso de revisión de envío de Amazon SES.

Cuando haya implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. Incluya detalles de las medidas que ha tomado para resolver este problema, así como detalles de sus planes para garantizar que este problema no se vuelva a producir. Una vez que recibamos su solicitud, revisaremos la información que ha proporcionado y cambiaremos el estado de su cuenta, si es necesario.

Notificación de sitio vulnerable

Esta sección contiene información adicional acerca de las notificaciones de sitio vulnerable mostradas en la página de métricas de reputación de Amazon SES.

¿Por qué ha recibido esta notificación?

Una revisión global ha encontrado que se envían mensajes desde su cuenta que no creemos que pretenda enviar. Los proveedores de bandeja de correo y los destinatarios marcarán muy probablemente estos mensajes como spam.

Con mucha frecuencia en estas situaciones, un tercero está abusando de una característica de su sitio web para enviar correo electrónico no deseado. Por ejemplo, si el sitio web contiene una función

"enviar por correo electrónico a un amigo", "póngase en contacto con nosotros", "invitar a un amigo" o similar, un tercero podría utilizar esta funcionalidad para enviar correo electrónico no solicitado.

Qué puede hacer para resolver el problema

En primer lugar, identifique las características de su sitio web o de sus aplicaciones que podrían permitir a terceros enviar correos electrónicos mediante Amazon SES sin su conocimiento. En el caso del Centro de soporte, puede solicitar una muestra de los mensajes que creemos que se enviaron de esta manera.

A continuación, modifique su aplicación o sitio web para evitar el envío no solicitado. Por ejemplo, añada un CAPTCHA, limite la velocidad a la que se pueden enviar correos electrónicos, elimine la posibilidad de que los usuarios envíen contenido personalizado, obligue a los usuarios a iniciar sesión para enviar correo electrónico y elimine la posibilidad de que la aplicación genere varias notificaciones simultáneas.

Si su cuenta está en proceso de revisión o se ha suspendido su capacidad para enviar correo electrónico

Cuando haya implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. Incluya detalles de las medidas que ha tomado para resolver este problema, así como detalles de sus planes para garantizar que este problema no se vuelva a producir. Una vez que recibamos su solicitud, revisaremos la información que ha proporcionado y cambiaremos el estado de su cuenta, si es necesario.

Si eliminamos el período de revisión o la suspensión del envío desde su cuenta y observamos el mismo problema más adelante, podríamos poner su cuenta en proceso de revisión o suspender su capacidad para enviar correo electrónico de nuevo. Si observamos casos extremos o el mismo problema repetidamente, podríamos suspender de forma permanente la capacidad de su cuenta para enviar correo electrónico.

Consulte Preguntas frecuentes acerca del proceso de revisión de envío de Amazon SES para obtener más información sobre qué hacer si su cuenta está en proceso de revisión o se ha suspendido su capacidad para enviar correo electrónico.

Notificación de credenciales comprometidas

Esta sección contiene información adicional acerca de las notificaciones del sitio de credenciales comprometidas mostradas en la página de métricas de reputación de Amazon SES.

¿Por qué ha recibido esta notificación?

Una revisión global ha encontrado que se envían mensajes desde su cuenta que no creemos que pretenda enviar. Los proveedores de bandeja de correo y los destinatarios marcarán muy probablemente estos mensajes como spam.

Algunas causas comunes son claves de acceso de IAM comprometidas, contraseñas SMTP comprometidas u otras vulnerabilidades de seguridad.

Qué puede hacer para resolver el problema

Debe realizar una revisión de seguridad exhaustiva de sus mecanismos de utilización de SES. Asegúrese de haber rotado las contraseñas SMTP o las contraseñas aplicables y de haber eliminado los usuarios o recursos no autorizados de la cuenta. Asegúrese de no almacenar información confidencial, como contraseñas o claves de acceso en sitios web o repositorios de terceros. Ahora se recomienda no utilizar claves de acceso de IAM para los usuarios y nunca para el usuario raíz. Si aún las usa, debe migrarlas a mecanismos que proporcionen credenciales temporales, como la creación de un usuario en AWS IAM Identity Center.

Si su cuenta está en proceso de revisión o se ha suspendido su capacidad para enviar correo electrónico

Cuando haya implementado los cambios que considera que resolverán el problema, inicie sesión en la consola de AWS y vaya al Centro de soporte. Responda al caso que abrimos en su nombre. Incluya detalles de las medidas que ha tomado para resolver este problema, así como detalles de sus planes para garantizar que este problema no se vuelva a producir. Una vez que recibamos su solicitud, revisaremos la información que ha proporcionado y cambiaremos el estado de su cuenta, si es necesario.

Si eliminamos el período de revisión o la suspensión del envío desde su cuenta y observamos el mismo problema más adelante, podríamos poner su cuenta en proceso de revisión o suspender su capacidad para enviar correo electrónico de nuevo. Si observamos casos extremos o el mismo problema repetidamente, podríamos suspender de forma permanente la capacidad de su cuenta para enviar correo electrónico.

Consulte Preguntas frecuentes acerca del proceso de revisión de envío de Amazon SES para obtener más información sobre qué hacer si su cuenta está en proceso de revisión o se ha suspendido su capacidad para enviar correo electrónico.

Otras notificaciones

Esta sección contiene información adicional acerca de otras notificaciones mostradas en la página de métricas de reputación de Amazon SES.

¿Por qué ha recibido esta notificación?

Una revisión automática o humana ha identificado problemas que no están incluidos en las secciones anteriores de este documento.

Qué puede hacer para resolver el problema

Consulte el caso del Centro de soporte que abrimos en su nombre para obtener más información sobre el problema específico. Para acceder al Centro de soporte, inicie sesión en la AWS Management Console y, a continuación, elija Centro de soporte. En su respuesta al caso, describa los cambios que implementó. Dependiendo de su situación específica y de la naturaleza de los problemas que descubramos, podríamos finalizar el periodo de revisión o restablecer la capacidad de su cuenta para enviar correo electrónico.

Creación de alarmas de monitoreo de reputación en CloudWatch

Amazon SES publica automáticamente una serie de métricas relacionadas con la reputación en Amazon CloudWatch. Puede utilizar estas métricas para crear alarmas que le avisarán cuando sus tasas de rebotes o reclamaciones alcancen niveles que podrían afectar a la capacidad de su cuenta de enviar correos electrónicos.

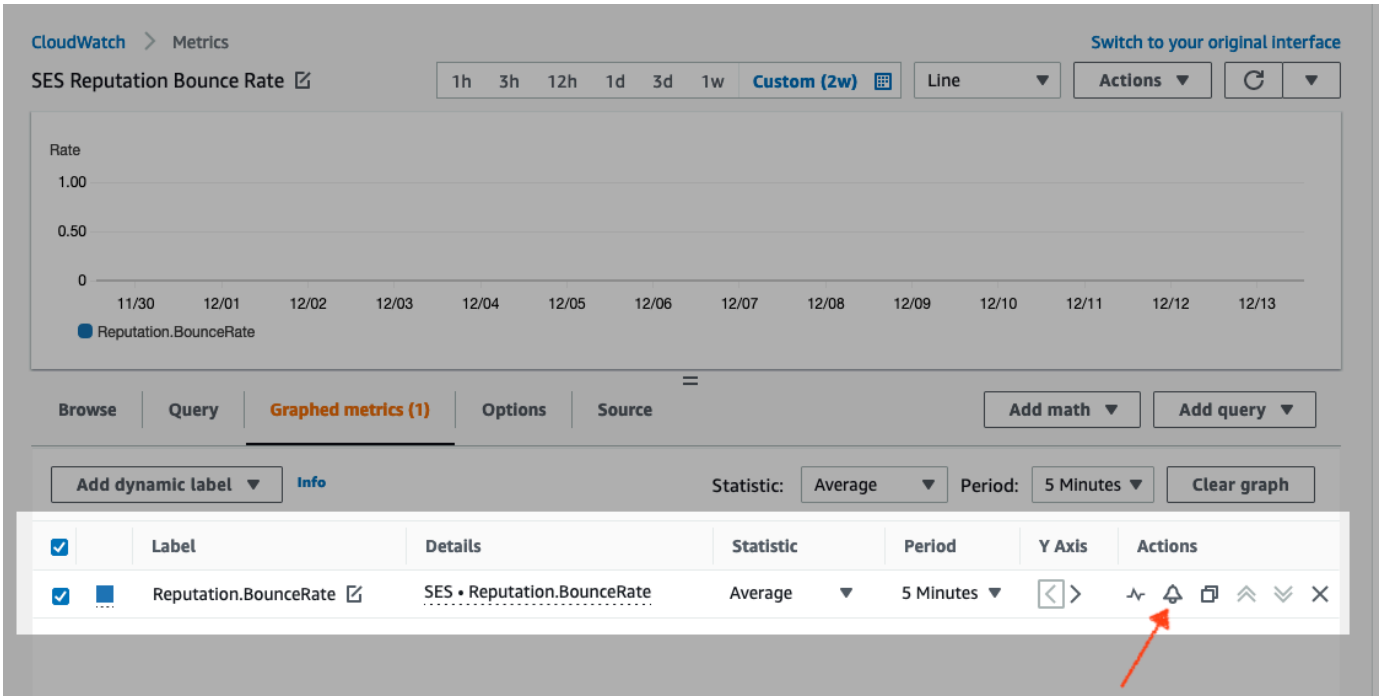
> **Note**
>
> La parte de CloudWatch de los procedimientos de esta sección pretende presentar los pasos principales para configurar una alarma de CloudWatch destinada a monitorear la reputación de su remitente SES. No se exploran configuraciones avanzadas con respecto a la configuración opcional de las alarmas de CloudWatch. Para obtener información completa acerca de la configuración de las alarmas de CloudWatch, consulte Uso de las alarmas de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

Requisitos previos

- Cree un tema de Amazon SNS y, a continuación, suscríbase a este utilizando su punto de conexión preferido (como, por ejemplo, correo electrónico o SMS). Para obtener más información, consulte Creación de un tema de Amazon SNS y Suscripción a un tema de Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.
- Si nunca ha enviado un correo electrónico en la región actual, es posible que no vea el espacio de nombres de SES. Para asegurarse de que tiene métricas, envíe un correo electrónico de prueba al simulador de buzón de correo.

Para crear una alarma de CloudWatch destinada a monitorear la reputación de los envíos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En el panel de navegación del lado izquierdo de la pantalla, elija Reputation metrics (Métricas de reputación).
3. En la página Métricas de reputación debajo de la pestaña Nivel de cuenta, ya sea en el panel Tasa de rebotes o Tasa de reclamaciones, elija Ver en CloudWatch, esto abrirá la consola de CloudWatch con la métrica elegida.
4. En la pestaña Graphed metrics (Representación gráfica de métricas), en la línea de la métrica elegida, para este ejemplo, Reputation.BounceRate, elija el icono de campana de alarma en la columna Actions (Acciones) (ver imagen a continuación): se abrirá la página Specify metrics and conditions (Especificar métrica y condiciones).



5. Desplácese hasta el panel Conditions (Condiciones) y elija Static (Estático) en el campo Threshold type (Tipo de umbral).

   a. En el campo Whenever ***`metric`*** is… (Siempre que la métrica sea…), elija Greater/Equal (Mayor/Igual).

   b. En el campo than… (que…), especifique el valor que debería provocar que CloudWatch active una alarma.

      - Si va a crear una alarma para monitorear la tasa de rebote, tenga en cuenta que Amazon SES recomienda mantener una tasa de rebotes por debajo del 5 %. Si la tasa de rebotes de su cuenta es mayor del 10%, podríamos suspender la capacidad de su cuenta para enviar correos electrónicos. Por este motivo, debe configurar CloudWatch para que le envíe una notificación cuando la tasa de rebotes de su cuenta sea mayor o igual al 0,05 (5 %).
      - Si va a crear una alarma para monitorear la tasa de reclamos, tenga en cuenta que Amazon SES recomienda mantener una tasa de reclamos por debajo del 0,1 %. Si la tasa de reclamaciones de su cuenta es mayor de 0,5%, podríamos suspender la capacidad de su cuenta para enviar correos electrónicos. Por este motivo, debe configurar CloudWatch para que le envíe una notificación cuando la tasa de reclamos de su cuenta sea mayor o igual a 0,001 (0,1 %).

c. Amplíe Additional configuration (Configuración adicional) y elija Treat missing data as ignore (maintain the alarm state) (Ignorar datos faltantes [mantener el estado de alarma]) en el campo Missing data treatment (Tratamiento de datos faltantes).

d. Elija Siguiente.

6. En el panel Configure actions (Configurar acciones), elija In Alarm (En alrama) en el campo Alarm state trigger (Activación de estado de alarma).

   a. Elija Select an existing SNS topic (Seleccionar un tema existente de SNS) en el campo Select an SNS topic (Seleccionar un tema de SNS).

   b. Elija un tema que haya creado y donde se haya suscrito en los requisitos previos en el cuadro de búsqueda Send a notification to… (Enviar una notificación a…).

   c. Elija Siguiente.

7. En el panel Add name and description (Agregar nombre y descripción), escriba un nombre y una descripción de la alarma y, a continuación, elija Next (Siguiente).

8. En el panel Preview and create (Vista previa y creación), confirme la configuración y, si está satisfecho, elija Create alarm (Crear alarma). Si hay algo que le gustaría cambiar, seleccione el botón Previous (Volver) de cada sección a la que desea regresar y realizar modificaciones.

Métricas de SNDS para direcciones IP dedicadas

Puede ver datos de Smart Network Data Services (SNDS) para direcciones IP dedicadas arrendadas en cada Región de AWS en la que utilice Amazon SES. Los datos de SNDS están disponibles mediante la consola de Amazon CloudWatch.

SNDS es un programa de Outlook que permite a los propietarios de direcciones IP ayudar a prevenir el spam en su espacio de IP. Amazon SES proporciona estos datos importantes para aquellos usuarios que arrendan direcciones IP dedicadas. Los datos de SNDS proporcionan información sobre el comportamiento de envío de correo de la dirección IP y señalan áreas problemáticas para la reputación del remitente.

> **Note**
>
> Con referencia a Outlook, abarca todos los dominios de los que realizan el seguimiento. Por ejemplo, esto puede abarcar Hotmail.com, Outlook.com y Live.com.

Para ver los datos de SNDS de las direcciones IP dedicadas

1. Inicie sesión en la consola de Amazon CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, expanda Metrics (Métricas) y elija All metrics (Todas las métricas).

   (Se proporcionan indicaciones para la nueva interfaz de consola de CloudWatch).
3. En la pestaña Browse (Navegar) del contenedor Metrics (Métricas), seleccione Región de AWS y, a continuación, elija SES.
4. Elija IP Metrics (Métricas de IP), que le mostrará todas las direcciones IP dedicadas de las que SNDS realiza el seguimiento.

   (Nota: si no hay direcciones IP dedicadas asociadas a la cuenta en la región seleccionada, IP Metrics (Métricas de IP) no aparecerá en la consola de CloudWatch).
5. Vea todas sus direcciones IP dedicadas de las que SNDS realiza el seguimiento en esta lista, o seleccione una dirección IP individual para ver solo sus métricas.

Las siguientes métricas se proporcionan para cada dirección IP dedicada y las define Outlook. Para obtener más información, consulte las preguntas frecuentes sobre SNDS de Outlook.

> **Note**
>
> Estas métricas representan un período de actividad que proporciona datos que se actualizan una vez al día. Las métricas también tienen una marca de tiempo correspondiente, que refleja un periodo de 24 horas.

- SNDS.RCPTCommands: es el número de comandos RCPT percibidos por SNDS para la dirección IP específica durante el periodo de actividad. Los comandos RCPT forman parte del protocolo SMTP utilizado para enviar correo, que especifica la dirección del destinatario a la que se intenta entregar el correo electrónico.
- SNDS.DATACommands: es el número de comandos DATA percibidos por SNDS para la dirección IP específica durante el periodo de actividad. Los comandos DATA forman parte del protocolo SMTP utilizado para enviar correo, específicamente la parte que realmente transmite el mensaje a los destinatarios previstos establecidos previamente.
- SNDS.MessageRecipients: número de destinatarios en los mensajes percibidos por SNDS para la dirección IP específica durante el periodo de actividad.

- SNDS.SpamRate: muestra los resultados agregados del filtrado de spam aplicado a todos los mensajes enviados por la dirección IP durante el periodo de actividad especificado.
  - Un valor de SpamRate de 0 significa que la dirección IP tiene menos del 10 % de spam.
  - Un valor de SpamRate de 0,5 significa que entre el 10 % y el 90 % de spam se genera a partir de la dirección IP.
  - Un valor de SpamRate de 1 significa que las tasas de spam del 90 % o más se generan a partir de la dirección IP.
- SNDS.ComplaintRate: fracción del tiempo que un usuario de Outlook realiza un reclamo de un mensaje recibido de la dirección IP durante el periodo de actividad.
  - Un valor de ComplaintRate de 1 significa una tasa de reclamos del 100 %.
  - Un valor de ComplaintRate de 0,05 significaría, por ejemplo, una tasa de reclamos del 5 %.
  - Un valor de ComplaintRate de 0 significa que la tasa es inferior al 0,1 %.
- SNDS.TrapHits: muestra el número de mensajes enviados a “cuentas trampa”. Las cuentas trampa son cuentas mantiene Outlook que no solicitan ningún correo. Por lo tanto, cualquier mensaje enviado a las cuentas trampa es muy probable que sea spam.

Preguntas de solución de problemas

Q1 (P1). ¿Por qué los datos no se rellenan todos los días? Podría aplicarse cualquiera de los siguientes escenarios:

- Los datos de SNDS dependen del programa SNDS de Outlook.
- Hay un umbral mínimo de correos electrónicos que SNDS necesita recibir para calcular un valor. Es posible que los datos no estén disponibles cuando el volumen de correo electrónico en una dirección IP es bajo.

Q2 (P2). ¿Por qué cambian las métricas de SNDS.SpamRate y SNDS.ComplaintRate, y qué hago si la tasa cambia a un valor de 1?

Este es un indicador de que algo en su comportamiento de envío ha desencadenado una respuesta negativa del programa SNDS de Outlook. En este caso, puede consultar a otros proveedores de servicios de Internet (ISP), así como a sus números de contacto, para asegurarse de que no se trata de un problema global. Si se trata de un problema global, es posible que vea problemas con varios ISP, lo que sugeriría un problema de lista, contenido, distribución o permisos. Si es específico de Outlook, revise el procedimiento óptimo de entrega a Outlook.

Q3 (P3). ¿Qué acciones realizará AWS Support si mi valor de SNDS.SpamRate cambia de 0 (o 0,5) a 1?

AWS no tiene ningún control sobre SNDS y, por lo tanto, no influye en este programa. Todas las solicitudes de mitigación deben presentarse directamente a Outlook a través de su nuevo formulario de solicitud de soporte.

Suspensión automática del envío de correo electrónico

Para proteger su reputación como remitente, puede suspender temporalmente el envío de correo electrónico para los mensajes enviados mediante conjuntos de configuración específicos o para todos los mensajes enviados desde su cuenta de Amazon SES en una región de AWS específica.

Mediante Amazon CloudWatch y Lambda, puede crear una solución que suspenda automáticamente el envío de correo electrónico cuando sus métricas de reputación (como la tasa de rebotes o de reclamos) superen determinados umbrales. Este tema contiene procedimientos para configurar esta solución.

Temas de esta sección:

- Poner en pausa automáticamente el envío de correo electrónico en toda su cuenta de Amazon SES
- Suspensión automática del envío de correos electrónicos para un conjunto de configuración

Poner en pausa automáticamente el envío de correo electrónico en toda su cuenta de Amazon SES

Los procedimientos de esta sección explican los pasos para configurar Amazon SES, Amazon SNS, Amazon CloudWatch y AWS Lambda para suspender automáticamente el envío de correo electrónico para una cuenta de Amazon SES de una sola región de AWS. Si envía correo electrónico desde varias regiones, repita los procedimientos de esta sección para cada región en la que desee implementar esta solución.

Temas de esta sección:

- Parte 1: crear un rol de IAM
- Parte 2: crear la función de Lambda
- Parte 3: volver a habilitar el envío de correos electrónicos en su cuenta

- Parte 4: Crear un tema de Amazon SNS y una suscripción
- Parte 5: crear una alarma de CloudWatch
- Parte 6: probar la solución

Parte 1: crear un rol de IAM

El primer paso para configurar la suspensión automática del envío de correo electrónico es crear un rol de IAM que pueda ejecutar la operación de la API `UpdateAccountSendingEnabled`.

Para crear el rol de IAM

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. Seleccione Roles en el panel de navegación.
3. Elija Create role (Crear rol).
4. En la página Select trusted entity (Seleccionar entidad de confianza), elija AWS service para el Trusted entity type (Tipo de entidad de confianza).
5. En Use case (Caso de uso), elija Lambda y, a continuación, elija Next (Siguiente).
6. En la página Add permissions (Agregar permisos), elija las siguientes políticas:

   - AWSLambdaBasicExecutionRole
   - AmazonSESFullAccess

   > **Tip**
   >
   > Utilice el cuadro de búsqueda en Permission policies (Políticas de permisos) para localizar rápidamente estas políticas, pero tenga en cuenta que después de buscar y seleccionar la primera política, debe elegir Clear filters (Borrar filtros) antes de buscar y seleccionar la segunda política.

   A continuación, elija Next.
7. En la página Name, review, and create (Nombre, revisión y crear), en Role details (Detalles de rol), ingrese un nombre con significado para la política en el campo Role name (Nombre de rol).
8. Compruebe que las dos políticas que ha seleccionado aparecen en la tabla Permissions policy summary (Resumen de la política de permisos) y, a continuación, elija Create role (Crear rol).

Parte 2: crear la función de Lambda

Después de crear un rol de IAM, puede crear la función de Lambda que suspende el envío de correo electrónico para la cuenta.

Para crear la función de Lambda

1. Abra la consola de AWS Lambda en https://console.aws.amazon.com/lambda/.
2. Utilice el selector de regiones para elegir la región en la que desea implementar esta función de Lambda.

   > **Note**
   >
   > Esta función solo detiene el envío de correo electrónico en la región de AWS que seleccione en este paso. Si envía correos electrónicos desde más de una región, repita los procedimientos de esta sección para cada región en la que desee suspender automáticamente el envío de correos electrónicos.

3. Elija Crear función.
4. En Create function (Crear función), elija Author from scratch (Autor desde cero).
5. En Basic information (Información básica), realice los siguientes pasos:

   - En Function name (Nombre de la función), escriba un nombre para la función Lambda.
   - Para Tiempo de ejecución, elija Node.js 18x (o la versión que se ofrece actualmente en la lista de selección).
   - Para Architecture (Arquitectura), conserve el valor predeterminado preseleccionado, x86_64.
   - En permisos expanda Change default execution role (Cambiar rol de ejecución predeterminado) y elija Use an existing role (Utilizar un rol existente).
   - Haga clic dentro del cuadro de la lista Existing role (Rol existente) y elija el rol de IAM que creó en the section called “Parte 1: crear un rol de IAM”.

   A continuación, seleccione Create function (Crear función).
6. En Code source (Código fuente), en el editor de código, pegue el siguiente código:

```
'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);
        }
    });
};
```

A continuación, elija Deploy (Implementar).

7. Seleccione Test (Probar). Si aparece la ventana Configure test event (Configurar prueba de evento), ingrese un nombre en el campo Event name (Nombre de evento) y, a continuación, elija Save (Guardar).
8. Expanda el contenedor de Test (Pruebas) y seleccione el nombre del evento que acaba de crear y, a continuación, elija Test (Pruebas).
9. La pestaña de Execution results (Resultados de la ejecución) aparecerá, justo debajo de ella y a la derecha, asegúrese de que se muestre `Status: Succeeded`. Si la función no se pudo ejecutar, haga lo siguiente:

   - Compruebe que el rol de IAM que creó en the section called “Parte 1: crear un rol de IAM” contiene las políticas correctas.
   - Compruebe que el código de la función de Lambda no contiene ningún error. El editor de código de Lambda resalta automáticamente los errores de sintaxis y otros posibles problemas.

Parte 3: volver a habilitar el envío de correos electrónicos en su cuenta

Un efecto secundario de probar la función de Lambda en the section called “Parte 2: crear la función de Lambda” es que el envío de correo electrónico de su cuenta de Amazon SES se suspende. En la mayoría de los casos, no conviene suspender el envío de la cuenta hasta que se desencadena la alarma de CloudWatch.

Los procedimientos de esta sección vuelven a habilitar el envío de correo electrónico en su cuenta de Amazon SES. Para completar estos procedimientos, debe instalar y configurar la AWS Command Line Interface. Para obtener más información, consulte la Guía del usuario de AWS Command Line Interface.

Para volver a habilitar el envío de correo electrónico

1. En la línea de comandos, escriba el siguiente comando para volver a habilitar el envío de correos electrónicos para su cuenta. Reemplace *sending_region* por el nombre de la región en la que desea volver a habilitar el envío de correos electrónicos.

   ```
   aws ses update-account-sending-enabled --enabled --region sending_region
   ```

2. En la línea de comandos, escriba el siguiente comando para verificar el estado del envío de correos electrónicos para su cuenta:

   ```
   aws ses get-account-sending-enabled --region sending_region
   ```

   Si ve el siguiente resultado, entonces ha vuelto a habilitar correctamente el envío de correos electrónicos en su cuenta:

   ```
   {
       "Enabled": true
   }
   ```

Parte 4: Crear un tema de Amazon SNS y una suscripción

Para que CloudWatch ejecute la función de Lambda cuando se desencadene una alarma, primero debe crear un tema de Amazon SNS y suscribir la función de Lambda a ese tema.

Para crear el tema de Amazon SNS y suscribirle la función de Lambda

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. Cree un tema siguiendo los pasos de la Guía para desarrolladores de Amazon Simple Notification Service.
   - El Type (Tipo) debe ser Standard (Estándar) (no FIFO).
3. Suscríbase al tema siguiendo los pasos de la Guía para desarrolladores de Amazon Simple Notification Service.
   a. En Protocol (Protocolo), elija AWS Lambda.
   b. En Endpoint (Punto de enlace), elija la función de Lambda que creó en the section called "Parte 2: crear la función de Lambda".

Parte 5: crear una alarma de CloudWatch

Esta sección contiene los procedimientos para crear una alarma de CloudWatch que se desencadena cuando una métrica alcanza un determinado umbral. Cuando se desencadena la alarma, se envía una notificación al tema de Amazon SNS que creó en the section called "Parte 4: Crear un tema de Amazon SNS y una suscripción", que a su vez ejecuta la función de Lambda que creó en the section called "Parte 2: crear la función de Lambda".

Para crear una alarma de CloudWatch

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. Utilice el selector de regiones para elegir la región en la que desea suspender automáticamente el envío de correos electrónicos.
3. En el panel de navegación, elija Alarms.
4. Elija Create Alarm (Crear alarma).
5. En la ventana Create Alarm (Crear alarma), en SES Metrics (Métricas de SES), elija Account Metrics (Métricas de la cuenta).
6. En Metric Name (Nombre de métrica), elija una de las siguientes opciones:
   - Reputation.BounceRate: elija esta métrica si desea poner en pausa el envío de correos electrónicos para su cuenta cuando el total de rechazos permanentes de su cuenta supere el umbral definido.

- Reputation.ComplaintRate: elija esta métrica si desea poner en pausa el envío de correos electrónicos para su cuenta cuando el total de reclamaciones de su cuenta supere el umbral definido.

Seleccione Next (Siguiente).

7. Realice los pasos siguientes:

   - En Alarm Threshold (Umbral de alarma), para Name (Nombre), escriba un nombre para la alarma.
   - En Whenever: Reputation.BounceRate o en Whenever: Reputation.ComplaintRate, especifique el umbral que provocará la activación de la alarma.

     > **Note**
     >
     > Su cuenta se pone automáticamente en proceso de revisión si la tasa de rebotes supera el 10 %, o si la tasa de reclamaciones supera el 0,5 %. Cuando especifique la tasa de rebotes o reclamos que hacen que se desencadene la alarma de CloudWatch, le recomendamos que utilice valores inferiores a estos porcentajes para evitar que su cuenta se ponga en proceso de revisión.

   - En Actions (Acciones), en Whenever this alarm (Siempre que esta alarma), elija State is ALARM (El estado es ALARMA). En Send notification to (Enviar notificación a), elija el tema de Amazon SNS que creó en the section called “Parte 4: Crear un tema de Amazon SNS y una suscripción”.

   Elija Create Alarm (Crear alarma).

Parte 6: probar la solución

Ahora puede probar la alarma para asegurarse de que se ejecuta la función de Lambda cuando entra en el estado `ALARM`. Puede utilizar la operación de la API `SetAlarmState` para cambiar temporalmente el estado de la alarma.

Los procedimientos de esta sección son opcionales, pero le recomendamos que los realice para asegurarse de que toda la solución está configurada correctamente.

1. En la línea de comandos, escriba el siguiente comando para verificar el estado del envío de correos electrónicos para su cuenta. Reemplace *region* por el nombre de la región.

   ```
   aws ses get-account-sending-enabled --region region
   ```

   Si el envío está activado para su cuenta, puede ver el siguiente resultado:

   ```
   {
       "Enabled": true
   }
   ```

2. En la línea de comandos, escriba el comando siguiente para cambiar temporalmente el estado de la alarma a ALARM: aws cloudwatch set-alarm-state --alarm-name ***MyAlarm*** --state-value ALARM --state-reason "Testing execution of Lambda function" --region ***region***

   Sustituya *MyAlarm* en el comando anterior por el nombre de la alarma que creó en la the section called “Parte 5: crear una alarma de CloudWatch” y sustituya *region* por la región en la que desea suspender automáticamente el envío de correo electrónico.

   > **Note**
   >
   > Cuando ejecute este comando, el estado de la alarma pasa de OK a ALARM y luego otra vez a OK al cabo de unos segundos. Puede ver estos cambios de estado en la pestaña History (Historial) de la alarma en la consola de CloudWatch o mediante la operación DescribeAlarmHistory.

3. En la línea de comandos, escriba el siguiente comando para verificar el estado del envío de correos electrónicos para su cuenta.

   ```
   aws ses get-account-sending-enabled --region region
   ```

   Si la función de Lambda se ha ejecutado correctamente, se muestra el resultado siguiente:

   ```
   {
       "Enabled": false
   }
   ```

4. Realice los pasos de the section called “Parte 3: volver a habilitar el envío de correos electrónicos en su cuenta” para volver a habilitar el envío de correos electrónicos en su cuenta.

Suspensión automática del envío de correos electrónicos para un conjunto de configuración

Puede configurar Amazon SES para exportar métricas de reputación específicas de los mensajes de correo electrónico enviados mediante un conjunto de configuración específico a Amazon CloudWatch. A continuación, puede utilizar estas métricas para crear alarmas de CloudWatch específicas de estos conjuntos de configuración. Cuando estas alarmas superen determinados umbrales, puede suspender automáticamente el envío de mensajes de correo electrónico que utilizan los conjuntos de configuración especificados, sin que esto afecte a las funcionalidades generales de envío de correo de su cuenta de Amazon SES.

> **Note**
>
> La solución que se describe en esta sección detiene el envío de correo electrónico para un conjunto de configuración específico de una sola región de AWS. Si envía correo electrónico desde varias regiones, repita los procedimientos de esta sección para cada región en la que desee implementar esta solución.

Temas de esta sección:

- Parte 1: habilitar los informes de métricas de reputación de un conjunto de configuración
- Parte 2: crear un rol de IAM
- Parte 3: crear la función de Lambda
- Parte 4: volver a habilitar el envío de correo electrónico para el conjunto de configuración
- Parte 5: crear un tema de Amazon SNS
- Parte 6: crear una alarma de CloudWatch
- Parte 7: probar la solución

Parte 1: habilitar los informes de métricas de reputación de un conjunto de configuración

Para poder configurar Amazon SES para suspender automáticamente el envío de correo electrónico para un conjunto de configuración, primero debe habilitar la exportación de métricas de reputación para el conjunto de configuración.

Para habilitar la exportación de métricas de rebotes y reclamaciones para el conjunto de configuración, realice los pasos de the section called “Ver y exportar métricas de reputación”.

Parte 2: crear un rol de IAM

El primer paso para configurar la suspensión automática del envío de correo electrónico es crear un rol de IAM que pueda ejecutar la operación de la API `UpdateConfigurationSetSendingEnabled`.

Para crear el rol de IAM

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. Seleccione Roles en el panel de navegación.
3. Elija Create role (Crear rol).
4. En Select type of trusted entity (Seleccionar tipo de entidad de confianza), elija AWS service (Servicio de AWS).
5. En Choose the service that will use this role (Elegir el servicio que usará este rol), elija Lambda. Elija Next: Permissions (Siguiente: permisos).
6. En la página Attach permissions policies (Adjuntar políticas de permisos), elija las siguientes políticas:

   - AWS LambdaBasicExecutionRole
   - AmazonSESFullAccess

   > **Tip**
   >
   > Utilice el cuadro de búsqueda de la parte superior de la lista de políticas para buscar rápidamente estas políticas.

   Elija Next: Review (Siguiente: revisar).
7. En la página Review (Revisar), en Name (Nombre), escriba un nombre para el rol. Elija Create role (Crear rol).

Parte 3: crear la función de Lambda

Después de crear un rol de IAM, puede crear la función de Lambda que suspende el envío de correo electrónico para el conjunto de configuración.

Para crear la función de Lambda

1. Abra la consola de AWS Lambda en https://console.aws.amazon.com/lambda/.
2. Utilice el selector de regiones para elegir la región en la que desea implementar esta función de Lambda.

   > **Note**
   >
   > Esta función solo detiene el envío de correo electrónico para los conjuntos de configuración de la región de AWS que seleccione en este paso. Si envía correos electrónicos desde más de una región, repita los procedimientos de esta sección para cada región en la que desee suspender automáticamente el envío de correos electrónicos.

3. Elija Crear función.
4. En Create function (Crear función), elija Author from scratch (Autor desde cero).
5. En Author from scratch (Autor desde cero), haga lo siguiente:

   - En Name (Nombre), escriba un nombre para la función de Lambda.
   - Para Runtime (Tiempo de ejecución), elija Node.js 14 x (o la versión que se ofrece actualmente en la lista de selección).
   - En Role (Rol), elija Choose an existing role (Elegir un rol existente).
   - En Existing role (Rol existente), elija el rol de IAM que creó en the section called “Parte 2: crear un rol de IAM”.

   Elija Crear función.

6. En Function code (Código de función), en el editor de código, pegue el código siguiente:

```
'use strict';

var aws = require('aws-sdk');
```

```
// Create a new SES object.
var ses = new aws.SES();

// Specify the parameters for this operation. In this example, you pass the
// Enabled parameter, with a value of false (Enabled = false disables email
// sending, Enabled = true enables it). You also pass the ConfigurationSetName
// parameter, with a value equal to the name of the configuration set for
// which you want to pause email sending.
var params = {
    ConfigurationSetName: ConfigSet,
    Enabled: false
};

exports.handler = (event, context, callback) => {
    // Pause sending for a configuration set
    ses.updateConfigurationSetSendingEnabled(params, function(err, data) {
        if(err) {
            console.log(err.message);
        } else {
            console.log(data);
        }
    });
};
```

Reemplace *ConfigSet* en el código anterior por el nombre del conjunto de configuración. Seleccione Save.

7. Seleccione Test (Probar). Si aparece la ventana Configure test event (Configurar prueba de evento), escriba un nombre en el campo Event name (Nombre de evento) y, a continuación, elija Create (Crear).
8. Asegúrese de que en la barra de notificación de la parte superior de la página se indica `Execution result: succeeded`. Si la función no se pudo ejecutar, haga lo siguiente:

   - Compruebe que el rol de IAM que creó en the section called “Parte 2: crear un rol de IAM” contiene las políticas correctas.
   - Compruebe que el código de la función de Lambda no contiene ningún error. El editor de código de Lambda resalta automáticamente los errores de sintaxis y otros posibles problemas.

Parte 4: volver a habilitar el envío de correo electrónico para el conjunto de configuración

Un efecto secundario de probar la función de Lambda en the section called “Parte 3: crear la función de Lambda” es que el envío de correo electrónico para el conjunto de configuración se suspende. En la mayoría de los casos, no conviene suspender el envío para el conjunto de configuración hasta que se activa la alarma de CloudWatch.

Los procedimientos de esta sección vuelven a habilitar el envío de correos electrónicos para su conjunto de configuración. Para completar estos procedimientos, debe instalar y configurar la AWS Command Line Interface. Para obtener más información, consulte la Guía del usuario de AWS Command Line Interface.

Para volver a habilitar el envío de correo electrónico

1. En la línea de comandos, escriba el siguiente comando para volver a habilitar el envío de correos electrónicos para el conjunto de configuración:

   ```
   aws ses update-configuration-set-sending-enabled \
   --configuration-set-name ConfigSet \
   --enabled
   ```

   En el comando anterior, sustituya *ConfigSet* por el nombre del conjunto de configuración para el que desea poner en pausa el envío de correo electrónico.

2. En la línea de comandos, escriba el siguiente comando para asegurarse de que el envío de correos electrónicos está habilitado:

   ```
   aws ses describe-configuration-set \
   --configuration-set-name ConfigSet \
   --configuration-set-attribute-names reputationOptions
   ```

   El comando genera resultados similares al siguiente ejemplo:

   ```
   {
       "ConfigurationSet": {
           "Name": "ConfigSet"
       },
       "ReputationOptions": {
           "ReputationMetricsEnabled": true,
   ```

```
        "SendingEnabled": true
    }
}
```

Si el valor de `SendingEnabled` es `true`, el envío de correos electrónicos para el conjunto de configuración se ha vuelto a habilitar correctamente.

Parte 5: crear un tema de Amazon SNS

Para que CloudWatch ejecute la función de Lambda cuando se desencadene una alarma, primero debe crear un tema de Amazon SNS y suscribir la función de Lambda a ese tema.

Para crear el tema de Amazon SNS

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. Utilice el selector de regiones para elegir la región en la que desea suspender automáticamente el envío de correos electrónicos.
3. En el panel de navegación, elija Topics (Temas).
4. Elija Create new topic (Crear nuevo tema).
5. En la ventana Create new topic (Crear nuevo tema), para Topic name (Nombre del tema), escriba un nombre para el tema. También puede incluir un nombre más descriptivo en el campo Display name (Mostrar nombre).

   Elija Create new topic (Crear nuevo nombre).
6. En la lista de temas, active la casilla situada junto al tema que creó en el paso anterior. En el menú Actions (Acciones), seleccione Subscribe to topic (Suscribirse al tema).
7. En la ventana Create subscription (Crear suscripción), seleccione estas opciones:
   - En Protocol (Protocolo), elija AWS Lambda.
   - En Endpoint (Punto de enlace), elija la función de Lambda que creó en the section called “Parte 3: crear la función de Lambda”.
   - En Version or alias (Versión o alias), elija default (predeterminado).
8. Seleccione Create subscription (Crear suscripción).

Parte 6: crear una alarma de CloudWatch

Esta sección contiene los procedimientos para crear una alarma de CloudWatch que se desencadena cuando una métrica alcanza un determinado umbral. Cuando se desencadena la alarma, se envía una notificación al tema de Amazon SNS que creó en the section called “Parte 5: crear un tema de Amazon SNS”, que a su vez ejecuta la función de Lambda que creó en the section called “Parte 3: crear la función de Lambda”.

Para crear una alarma de CloudWatch

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. Utilice el selector de regiones para elegir la región en la que desea suspender automáticamente el envío de correos electrónicos.
3. En el panel de navegación de la izquierda, elija Alarms (Alarmas).
4. Elija Create Alarm (Crear alarma).
5. En la ventana Create Alarm (Crear alarma), en SES Metrics (Métricas de SES), elija Configuration Set Metrics (Métricas de conjunto de configuración).
6. En la columna ses:configuration-set, busque el conjunto de configuración para el que desea crear una alarma. En Metric Name (Nombre de métrica), elija una de las siguientes opciones:

   - Reputation.BounceRate: elija esta métrica si desea poner en pausa el envío de correos electrónicos para el conjunto de configuración cuando el total de rechazos permanentes del conjunto de configuración supere el umbral definido.
   - Reputation.ComplaintRate: elija esta métrica si desea poner en pausa el envío de correos electrónicos para el conjunto de configuración cuando el total de reclamaciones del conjunto de configuración supere el umbral definido.

   Seleccione Next (Siguiente).
7. Realice los pasos siguientes:

   - En Alarm Threshold (Umbral de alarma), para Name (Nombre), escriba un nombre para la alarma.
   - En Whenever: Reputation.BounceRate o en Whenever: Reputation.ComplaintRate, especifique el umbral que provocará la activación de la alarma.

> **Note**
>
> Si la tasa de rebotes de su cuenta de Amazon SES supera el 10 % o si la tasa de reclamos total de su cuenta de Amazon SES supera el 0,5 %, su cuenta de Amazon SES se pone automáticamente en proceso de revisión. Cuando especifique la tasa de rebotes o reclamos que hacen que se desencadene la alarma de CloudWatch, le recomendamos que utilice valores muy inferiores a estos porcentajes para evitar que su cuenta se ponga en proceso de revisión.

- En Actions (Acciones), en Whenever this alarm (Siempre que esta alarma), elija State is ALARM (El estado es ALARMA). En Send notification to (Enviar notificación a), elija el tema de Amazon SNS que creó en the section called “Parte 5: crear un tema de Amazon SNS”.

Elija Create Alarm (Crear alarma).

Parte 7: probar la solución

Ahora puede probar la alarma para asegurarse de que se ejecuta la función de Lambda cuando entra en el estado `ALARM`. Puede utilizar la operación `SetAlarmState` de la API de CloudWatch para cambiar temporalmente el estado de la alarma.

Los procedimientos de esta sección son opcionales, pero le recomendamos que los realice para comprobar que toda la solución está configurada correctamente.

Para probar la solución

1. En la línea de comandos, escriba el siguiente comando para comprobar el estado del envío de correos electrónicos para el conjunto de configuración:

```
aws ses describe-configuration-set --configuration-set-name ConfigSet
```

Si el envío está habilitado para el conjunto de configuración, se muestra el resultado siguiente:

```
{
    "ConfigurationSet": {
        "Name": "ConfigSet"
    },
    "ReputationOptions": {
```

```
        "ReputationMetricsEnabled": true,
        "SendingEnabled": true
    }
}
```

Si el valor de `SendingEnabled` es `true`, el envío de correos electrónicos está habilitado actualmente para el conjunto de configuración.

2. En la línea de comandos, escriba el comando siguiente para cambiar temporalmente el estado de la alarma a `ALARM`:

```
aws cloudwatch set-alarm-state \
--alarm-name MyAlarm \
--state-value ALARM \
--state-reason "Testing execution of Lambda function"
```

Reemplace *`MiAlarma`* en el comando anterior por el nombre de la alarma que creó en the section called “Parte 6: crear una alarma de CloudWatch”.

> **Note**
>
> Cuando ejecute este comando, el estado de la alarma pasa de `OK` a `ALARM` y luego otra vez a `OK` al cabo de unos segundos. Puede ver estos cambios de estado en la pestaña History (Historial) de la alarma en la consola de CloudWatch o mediante la operación DescribeAlarmHistory.

3. En la línea de comandos, escriba el siguiente comando para comprobar el estado del envío de correos electrónicos para el conjunto de configuración:

```
aws ses describe-configuration-set \
--configuration-set-name ConfigSet
```

Si la función de Lambda se ejecutó correctamente, verá un resultado similar al siguiente ejemplo:

```
{
    "ConfigurationSet": {
        "Name": "ConfigSet"
    },
    "ReputationOptions": {
```

```
        "ReputationMetricsEnabled": true,
        "SendingEnabled": false
    }
}
```

Si el valor de `SendingEnabled` es `false`, el envío de correo electrónico para el conjunto de configuración se desactiva, lo que indica que la función de Lambda se ha ejecutado correctamente.

4. Realice los pasos de the section called “Parte 4: volver a habilitar el envío de correo electrónico para el conjunto de configuración” para volver a habilitar el envío de correos electrónicos para el conjunto de configuración.

Supervisión de eventos de SES con Amazon EventBridge

EventBridge es un servicio sin servidor que utiliza eventos para conectar los componentes de la aplicación, lo que facilita la creación de aplicaciones escalables basadas en eventos. La arquitectura basada en eventos es un estilo de creación de sistemas de software de acoplamiento flexible que funcionan juntos emitiendo eventos y respondiendo a ellos. Los eventos son mensajes con formato JSON que, por lo general, representan un cambio en un recurso o entorno u otro evento de administración.

Algunas funciones de SES generan y envían eventos al bus de eventos EventBridge predeterminado. Un bus de eventos es un enrutador que recibe eventos y los envía a cero o más destinos u objetivos. Las reglas que se asocian al bus de eventos evalúan los eventos a medida que llegan. Cada regla comprueba si un evento coincide con el patrón de la regla. Si el evento coincide, EventBridge envía el evento a los destinos especificados.

SES envía los eventos EventBridge cuando una función tiene un cambio de estado o una actualización de estado. Puede usar EventBridge reglas para dirigir los eventos a sus objetivos definidos. Estos eventos se entregarán según el mejor esfuerzo y pueden entregarse sin ordenar.

Temas

- Eventos de SES
- Referencia del esquema de eventos de SES
- Se utiliza EventBridge con eventos de SES
- EventBridge Recursos adicionales

Eventos de SES

Las funciones de SES generan los siguientes eventos y los envían al bus de eventos predeterminado EventBridge. Para obtener más información, incluidos los datos detallados de cada tipo de evento, consulte???.

Eventos de asesoramiento de Virtual Deliverability Manager

Tipo de evento	Descripción
Estado de recomendación de un asesor abierto	Un evento generado cada vez que se abre una nueva recomendación en el asesor del Administrador virtual de entrega.
Estado de recomendación de un asesor resuelto	Un evento generado cada vez que se resuelve una recomenda ción en el asesor del Administrador virtual de entrega.

Eventos de envío de correo electrónico de SES

Tipo de evento	Descripción
Correo electrónico devuelto	Un rebote forzoso de que el servidor de correo del destinatario rechazó permanentemente el correo electrónico. (Las devolucio nes temporales solo se incluyen cuando SES no puede entregar el correo electrónico tras intentarlo durante un tiempo).
Se hizo clic en el correo electrónico	El destinatario hizo clic en uno o más enlaces del correo electrónico.
Se recibió una queja por correo electrónico	El correo electrónico se envió correctamente al servidor de correo del destinatario, pero el destinatario lo marcó como correo no deseado.
Entrega de correo electrónico	SES entregó correctamente el correo electrónico al servidor de correo del destinatario.
Se retrasó la entrega del correo	No se pudo entregar el correo electrónico al servidor de correo del destinatario porque se produjo un problema temporal. Pueden producirse retrasos en la entrega, por ejemplo, si la bandeja de entrada del destinatario está llena o el servidor de recepción de email experimenta un problema transitorio.
Correo electrónico abierto	El destinatario recibió el mensaje y lo abrió en su cliente de correo electrónico.

Tipo de evento	Descripción
Correo electrónico rechazado	SES aceptó el correo electrónico, pero determinó que contenía un virus y no intentó entregarlo al servidor de correo del destinatario.
Falló la representación del correo electrónico	El correo electrónico no se envió debido a un problema de representación de la plantilla. Este tipo de evento se puede producir cuando faltan datos en la plantilla o cuando los parámetros y los datos de la plantilla no coinciden. (Este tipo de evento solo se produce cuando envía correo electrónico con las operaciones de la API `SendTemplatedEmail` o `SendBulkTemplatedEmail`).
Correo electrónico enviado	El envío de la solicitud se realizó correctamente y SES intentará entregar el mensaje al servidor de correo del destinatario. (Si se está utilizando la supresión global o de nivel de cuenta, SES lo seguirá contando como un envío, pero la entrega se suprimirá).
Correo electrónico suscrito	El correo electrónico se envió correctamente, pero el destinatario actualizó las preferencias de suscripción haciendo clic `List-Unsubscribe` en el encabezado del correo electrónico o en el `Unsubscribe` enlace del pie de página.

Referencia del esquema de eventos de SES

Todos los eventos de los AWS servicios tienen un conjunto común de campos que contienen metadatos sobre el evento, como el AWS servicio que lo origina, la hora en que se generó el evento, la cuenta y la región en las que tuvo lugar, entre otros. Para ver las definiciones de estos campos generales, consulte la referencia a la estructura de eventos en la Guía del EventBridge usuario.

Además, cada evento tiene un campo `detail` que contiene datos específicos de ese evento en particular. La siguiente referencia define los campos de detalle de los distintos eventos de SES.

Cuando se utilice EventBridge para seleccionar y gestionar eventos de SES, es útil tener en cuenta lo siguiente:

- El campo `source` para todos los eventos de SES está establecido en `aws.ses`.

- El campo `detail-type` especifica el tipo de evento. Consulte la tabla de tipos de eventos enthe section called “Eventos de SES”.
- El campo `detail` contiene los datos específicos de ese evento en particular.

  Para algunos tipos de eventos, como los de Virtual Deliverability Manager, el campo de detalle es una cadena de datos bastante simplista que se rellena a partir de un conjunto finito de valores estáticos. Por el contrario, el campo de detalle de los eventos de envío de correo electrónico es más complejo, ya que puede constar de muchos subcampos de detalle que son una combinación de valores estáticos y dinámicos, como la marca de tiempo del envío de un correo electrónico, la dirección del destinatario y muchos otros atributos del correo electrónico.

Temas

- Esquema de estado de asesor del Administrador virtual de entrega
- Esquema de estado de envío de correo electrónico de SES

Esquema de estado de asesor del Administrador virtual de entrega

La siguiente referencia de esquema define los campos específicos de los eventos de estado de asesor de Virtual Deliverability Manager.

Las definiciones de los campos generales que aparecen en todos los esquemas de eventos (como`version`, `idaccount`, y otros) se encuentran en la referencia a la estructura de eventos de la Guía del EventBridge usuario. Los campos `source` y `detail-type` se incluyen en la referencia siguiente porque contienen valores específicos de SES para los eventos de SES.

`source`

Identifica el servicio que generó el evento. Para los eventos de SES, este valor es `aws.ses`.

`detail-type`

Identifica el tipo de evento.

Los valores de este campo se muestran en la tabla de eventos del asesor de Virtual Deliverability Manager en. the section called “Eventos de SES”

`detail`

Un objeto JSON que contiene información sobre el evento. El servicio que genera el evento determina el contenido de este campo.

Los valores de este campo pueden ser:

- `DKIM verification is not enabled.`
- `DKIM verification has failed.`
- `DKIM signing key length is below 2048 bits.`
- `DMARC configuration was not found.`
- `DMARC configuration could not be parsed.`
- `DKIM record was not found.`
- `DKIM record is not aligned.`
- `MAIL FROM record is not aligned.`
- `SPF record was not found.`
- `SPF record for Amazon SES was not found.`
- `SPF all qualifier is missing.`
- `An SPF configuration issue was found.`
- `BIMI record not found or configured without default selector.`
- `BIMI has malformed TXT record.`

Example Ejemplo: evento de estado de asesor del Administrador virtual de entrega

A continuación, se muestra un ejemplo de un evento de estado de asesor del Administrador virtual de entrega para el tipo de evento `Advisor Recommendation Status Open`. El valor del evento detallado en este ejemplo es`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." }
```

```
}
```

Esquema de estado de envío de correo electrónico de SES

La siguiente referencia de esquema define los campos específicos de los eventos de estado de envío de correo electrónico de SES.

Las definiciones de los campos generales que aparecen en todos los esquemas de eventos (como`version`, `idaccount`, y otros) se encuentran en la referencia a la estructura de eventos de la Guía del EventBridge usuario. Los campos `source` y `detail-type` se incluyen en la referencia siguiente porque contienen valores específicos de SES para los eventos de SES.

`source`

Identifica el servicio que generó el evento. Para los eventos de SES, este valor es `aws.ses`.

`detail-type`

Identifica el tipo de evento.

Los valores de este campo se muestran en la tabla de eventos de envío de correo electrónico de SES enthe section called “Eventos de SES”.

`detail`

Un objeto JSON que contiene información sobre el evento. El servicio que genera el evento determina el contenido de este campo.

No se pueden enumerar aquí todos los valores posibles de este campo porque se componen de valores estáticos y dinámicos generados por cada correo electrónico único que se envía en un momento dado. Sin embargo, se proporciona un ejemplo para darle una idea del tipo de datos que puede contener este campo. Puede encontrar ejemplos de datos detallados para todos los tipos de eventos de envío de correo electrónico utilizando el EventBridge Sandbox, consulteEspecifique un ejemplo de evento en EventBridge.

Un ejemplo de datos detallados generados para el evento `Email Rendering Failed` de envío de correos electrónicos de SES:

```
...,
  "detail": {
    "eventType": "Rendering Failure",
    "mail": {
```

```
      "timestamp": "2018-01-22T18:43:06.197Z",
      "source": "sender@example.com",
      "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
      "sendingAccountId": "123456789012",
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
      "destination": ["recipient@example.com"],
      "headersTruncated": false,
      "tags": {
        "ses:configuration-set": ["ConfigSet"]
      }
    },
    "failure": {
      "errorMessage": "Attribute 'attributeName' is not present in the rendering
  data.",
      "templateName": "MyTemplate"
    }
  }
```

Example Ejemplo: evento de estado de envío de correo electrónico

El siguiente es un ejemplo del evento de estado completo del envío de correo electrónico para el tipo de eventoEmail Rendering Failed. El valor detallado del evento de este ejemplo es una combinación de valores estáticos y dinámicos basados en el evento de envío de correo electrónico de un correo electrónico específico.

```
{
  "version": "0",
  "id": "12a18625-3328-fafd-2809-a5e16004f112",
  "detail-type": "Email Rendering Failed",
  "source": "aws.ses",
  "account": "123456789012",
  "time": "2023-07-17T16:48:05Z",
  "region": "us-east-1",
  "resources": ["arn:aws:ses:us-east-1:123456789012:identity/example.com"],
  "detail": {
    "eventType": "Rendering Failure",
    "mail": {
      "timestamp": "2018-01-22T18:43:06.197Z",
      "source": "sender@example.com",
      "sourceArn": "arn:aws:ses:us-east-1:123456789012:identity/sender@example.com",
      "sendingAccountId": "123456789012",
      "messageId": "EXAMPLE7c191be45-e9aedb9a-02f9-4d12-a87d-dd0099a07f8a-000000",
```

```
      "destination": ["recipient@example.com"],
      "headersTruncated": false,
      "tags": {
        "ses:configuration-set": ["ConfigSet"]
      }
    },
    "failure": {
      "errorMessage": "Attribute 'attributeName' is not present in the rendering
 data.",
      "templateName": "MyTemplate"
    }
  }
}
```

Se utiliza EventBridge con eventos de SES

De forma predeterminada, SES envía los eventos al bus de eventos EventBridge predeterminado. Puede crear reglas en el bus de eventos predeterminado para identificar eventos específicos y enviarlos EventBridge a uno o más destinos específicos. Cada regla contiene un patrón de eventos que se EventBridge utiliza para hacer coincidir los eventos a medida que llegan al bus de eventos. Si un evento coincide con el patrón de eventos de una regla determinada, EventBridge envía el evento al destino especificado en la regla.

En EventBridge, definir un patrón de eventos suele formar parte de un proceso más amplio de crear una nueva regla o editar una existente. Para obtener información sobre cómo crear EventBridge reglas, consulta Cómo crear EventBridge reglas de Amazon que reaccionen a los eventos en la Guía del EventBridge usuario.

Al utilizar la función Sandbox EventBridge, puedes definir rápidamente un patrón de eventos y usar un evento de muestra para confirmar que el patrón coincide con los eventos deseados, sin tener que crear o editar primero una regla. Para obtener instrucciones detalladas sobre el uso del Sandbox, consulte Probar un patrón de eventos con el EventBridge Sandbox en la Guía del EventBridge usuario.

Especifique un ejemplo de evento de SES en el entorno aislado EventBridge

Puede seleccionar eventos de ejemplo para los eventos de SES y usarlos para probar los patrones de eventos que cree.

Para especificar un evento de ejemplo de SES en el EventBridge entorno aislado

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. En el panel de navegación, seleccione Recursos para desarrolladores, a continuación, seleccione Entorno aislado y, en la página Entorno aislado, seleccione la pestaña Patrón de eventos.
3. En Fuente del evento, selecciona AWS eventos o eventos EventBridge asociados.
4. En la sección Evento de muestra, en Tipo de evento de muestra, seleccione Eventos de AWS .
5. Para ver Eventos de ejemplo, desplácese hacia abajo hasta SES y, a continuación, seleccione el evento de SES deseado.

   EventBridge muestra un evento de muestra, junto con todos sus datos detallados, para el tipo de evento.

   A continuación, puede utilizar este evento para probar el patrón de eventos que ha creado en la sección Patrones de eventos o utilizarlo como base para crear sus propios eventos de muestra para las pruebas de patrones que se describen en la siguiente sección.

Creación y prueba de patrones de eventos para los eventos de SES

Una vez que hayas seleccionado un evento de ejemplo, como se ha explicado en la sección anterior, puedes crear un patrón de eventos y usar el evento de muestra para asegurarte de que coincide con los eventos que desees.

Para crear y probar un patrón de eventos que coincida con los eventos de SES en el EventBridge entorno aislado

1. Abre la EventBridge consola de Amazon en https://console.aws.amazon.com/events/.
2. En el panel de navegación, seleccione Recursos para desarrolladores, a continuación, seleccione Entorno aislado y, en la página Entorno aislado, seleccione la pestaña Patrón de eventos.
3. En Origen del evento, elige AWS eventos o eventos EventBridge asociados y selecciona el evento de muestra que quieres probar, tal y como se explica en la sección anterior.
4. Desplázate hacia abajo hasta Método de creación y selecciona Usar forma de patrón.
5. En la sección Patrón de eventos, en Fuente de eventos, elija Servicios de AWS .
6. En AWS Servicio, selecciona SES.

7. Para Tipo de evento, seleccione el tipo de evento de SES que desea emparejar.

   EventBridge muestra el patrón de eventos mínimo, compuesto por `detail-type` campos `source` y campos, que coincide con el evento SES seleccionado.

   En los dos ejemplos, el primer patrón de eventos coincide con todos los `Advisor Recommendation Status Resolved` eventos y, en el segundo, con todos los `Email Bounced` eventos:

   ```
   {
     "source": ["aws.ses"],
     "detail-type": ["Advisor Recommendation Status Resolved"]
   }
   ```

   ```
   {
     "source": ["aws.ses"],
     "detail-type": ["Email Bounced"]
   }
   ```

8. Para realizar cambios en el patrón de eventos, selecciona Editar patrón y realiza los cambios en el editor JSON.

   También puede hacer coincidir los valores de uno o más campos de datos de detalle. Esto incluye especificar varios valores posibles para un valor de campo.

   En el siguiente ejemplo, se agregó el campo de detalle al patrón de eventos mínimo generado con el valor de `data` campo especificado como `DKIM record was not found` para buscar todos los eventos de los asesores de Virtual Deliverability Manager con el mismo valor de detalle:

   ```
   {
     "source": ["aws.ses"],
     "detail-type": ["Advisor Recommendation Status Resolved"],
     "detail": {
       "data": ["DKIM record was not found."]
     }
   }
   ```

   En este ejemplo, se agregaron subcampos de detalles para informar sobre los eventos generados por todos los correos electrónicos enviados desde noreply@example.com el 5 de

agosto de 2020 y que fueron rechazados. (La coincidencia de prefijos se utiliza aquí como parte del filtrado de contenido.):

```
{
  "source": ["aws.ses"],
  "detail-type": ["Email Bounced"],
  "detail": {
    "mail": {
      "timestamp": [{
        "prefix": "2024-08-05"
      }],
      "source": ["noreply@example.com"]
    }
  }
}
```

Es importante que leas los patrones de eventos en la Guía del EventBridge usuario, donde se explica que el valor del patrón de eventos que introduzcas en el editor JSON debe estar entre corchetes `[...]` porque se considera una matriz. También se proporciona esta y más información sobre cómo crear patrones de eventos avanzados.

9. Para comprobar si su patrón de eventos coincide con el evento de ejemplo que especificó en el panel de eventos de ejemplo anterior, seleccione Probar patrón. Si coincide, aparecerá un cartel verde en la parte inferior del editor JSON: «El evento de muestra coincidió con el patrón del evento».
10. Para solucionar errores tras seleccionar el patrón de prueba:

    - Si hay errores relacionados con JSON, el mensaje indicará el motivo, por ejemplo: «El patrón de eventos no es válido». Motivo: los «datos» deben ser un objeto o una matriz en la línea: 5, columna: 14». Para solucionar este problema, coloque el valor en la línea 5 entre corchetes. `[...]`
    - Si hay una discrepancia entre los valores del evento de muestra y tu patrón de eventos, el mensaje será: «El evento de muestra no coincidió con el patrón de eventos». Esto significa que uno o más valores que quieres probar son diferentes de los valores de ejemplo generados por el generador de eventos de Sample. Para solucionar este problema, continúe con los pasos restantes.
11. Para cambiar los valores de muestra en el evento de muestra con el fin de probar correctamente el patrón de eventos, en el panel de eventos de muestra, selecciona Copiar en el editor JSON.

12. Selecciona el botón de radio situado junto al tipo de evento Enter my own for Sample situado en la parte superior del editor.
13. Pegue el evento de ejemplo en el editor JSON y, en cualquier campo que utilice en su patrón de eventos, sustituya el valor de ese mismo campo para que coincida con el valor que especificó en su patrón de eventos.
14. Desplázate hacia abajo hasta el panel Patrón de eventos y vuelve a seleccionar Probar patrón. Si todos los valores se introdujeron correctamente y coinciden, aparecerá un cartel verde en la parte inferior del editor JSON que dice: «El evento de muestra coincidió con el patrón de eventos».

EventBridge Recursos adicionales

Consulta los siguientes temas de la Guía del EventBridge usuario de Amazon para obtener más información sobre EventBridge cómo procesar y gestionar eventos.

- Para obtener información detallada sobre cómo funcionan los autobuses de eventos, consulta Amazon EventBridge Event Bus.
- Para obtener información sobre la estructura de los eventos, consulte Events.
- Para obtener información sobre cómo crear patrones de eventos EventBridge para usarlos al comparar eventos con las reglas, consulte Patrones de eventos
- Para obtener información sobre la creación de reglas para especificar qué eventos se EventBridge procesan, consulte Reglas
- Para obtener información sobre cómo especificar a qué servicios u otros destinos EventBridge envían los eventos coincidentes, consulte Targets

Ejemplos de código de Amazon SES con SDK de AWS

Los siguientes ejemplos de código muestran cómo utilizar Amazon SES con un kit de desarrollo de software (SDK) de AWS.

Para obtener una lista completa de las guías para desarrolladores del SDK de AWS y ejemplos de código, consulte Uso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Ejemplos de código

- Ejemplos de código para Amazon SES con AWS SDK
  - Acciones para Amazon SES mediante AWS SDK
    - Úselo CreateReceiptFilter con un AWS SDK o CLI
    - Úselo CreateReceiptRule con un AWS SDK o CLI
    - Úselo CreateReceiptRuleSet con un AWS SDK o CLI
    - Úselo CreateTemplate con un AWS SDK o CLI
    - Úselo DeleteIdentity con un AWS SDK o CLI
    - Úselo DeleteReceiptFilter con un AWS SDK o CLI
    - Úselo DeleteReceiptRule con un AWS SDK o CLI
    - Úselo DeleteReceiptRuleSet con un AWS SDK o CLI
    - Úselo DeleteTemplate con un AWS SDK o CLI
    - Úselo DescribeReceiptRuleSet con un AWS SDK o CLI
    - Úselo GetIdentityVerificationAttributes con un AWS SDK o CLI
    - Úselo GetSendQuota con un AWS SDK o CLI
    - Úselo GetSendStatistics con un AWS SDK o CLI
    - Úselo GetTemplate con un AWS SDK o CLI
    - Úselo ListIdentities con un AWS SDK o CLI
    - Úselo ListReceiptFilters con un AWS SDK o CLI
    - Úselo ListTemplates con un AWS SDK o CLI
    - Úselo SendBulkTemplatedEmail con un AWS SDK o CLI
    - Úselo SendEmail con un AWS SDK o CLI
    - Úselo SendRawEmail con un AWS SDK o CLI

- Úselo SendTemplatedEmail con un AWS SDK o CLI
- Úselo UpdateTemplate con un AWS SDK o CLI
- Úselo VerifyDomainIdentity con un AWS SDK o CLI
- Úselo VerifyEmailIdentity con un AWS SDK o CLI

- Escenarios para Amazon SES con AWS SDK
  - Copie las identidades de correo electrónico y dominio de Amazon SES de una AWS región a otra mediante un AWS SDK
  - Generación de credenciales para conectarse a un punto de conexión SMTP de Amazon SES
  - Verificar la identidad de un correo electrónico y enviar mensajes con Amazon SES mediante un AWS SDK
- Ejemplos de servicios cruzados para Amazon SES que utilizan SDK AWS
  - Creación de una aplicación de streaming de Amazon Transcribe
  - Creación de una aplicación web para hacer un seguimiento de los datos de DynamoDB
  - Crear un rastreador de artículos de Amazon Redshift
  - Crear un rastreador de elementos de trabajo de Aurora Serverless
  - Detecte el PPE en las imágenes con Amazon Rekognition AWS mediante un SDK
  - Detecte objetos en imágenes con Amazon Rekognition AWS mediante un SDK
  - Detecte personas y objetos en un vídeo con Amazon Rekognition AWS mediante un SDK
  - Uso de Step Functions para invocar funciones de Lambda

- Ejemplos de código para la API v2 de Amazon SES con AWS SDK
  - Acciones para la API v2 de Amazon SES mediante AWS SDK
    - Úselo CreateContact con un AWS SDK o CLI
    - Úselo CreateContactList con un AWS SDK o CLI
    - Úselo CreateEmailIdentity con un AWS SDK o CLI
    - Úselo CreateEmailTemplate con un AWS SDK o CLI
    - Úselo DeleteContactList con un AWS SDK o CLI
    - Úselo DeleteEmailIdentity con un AWS SDK o CLI
    - Úselo DeleteEmailTemplate con un AWS SDK o CLI
    - Úselo GetEmailIdentity con un AWS SDK o CLI
    - Úselo ListContactLists con un AWS SDK o CLI

- Úselo ListContacts con un AWS SDK o CLI
- Úselo SendEmail con un AWS SDK o CLI

- Escenarios para la API v2 de Amazon SES con AWS SDK
  - Un flujo de trabajo completo para el boletín de Amazon SES API v2 mediante un AWS SDK

Ejemplos de código para Amazon SES con AWS SDK

Los siguientes ejemplos de código muestran cómo usar Amazon SES con un kit de desarrollo de AWS software (SDK).

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las funciones de servicio individuales, es posible ver las acciones en contexto en los escenarios relacionados y en los ejemplos entre servicios.

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica llamando a varias funciones dentro del mismo servicio.

Los ejemplos con varios servicios son aplicaciones de muestra que funcionan con varios Servicios de AWS.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Ejemplos de código

- Acciones para Amazon SES mediante AWS SDK
  - Úselo CreateReceiptFilter con un AWS SDK o CLI
  - Úselo CreateReceiptRule con un AWS SDK o CLI
  - Úselo CreateReceiptRuleSet con un AWS SDK o CLI
  - Úselo CreateTemplate con un AWS SDK o CLI
  - Úselo DeleteIdentity con un AWS SDK o CLI
  - Úselo DeleteReceiptFilter con un AWS SDK o CLI
  - Úselo DeleteReceiptRule con un AWS SDK o CLI
  - Úselo DeleteReceiptRuleSet con un AWS SDK o CLI
  - Úselo DeleteTemplate con un AWS SDK o CLI

- Úselo DescribeReceiptRuleSet con un AWS SDK o CLI
- Úselo GetIdentityVerificationAttributes con un AWS SDK o CLI
- Úselo GetSendQuota con un AWS SDK o CLI
- Úselo GetSendStatistics con un AWS SDK o CLI
- Úselo GetTemplate con un AWS SDK o CLI
- Úselo ListIdentities con un AWS SDK o CLI
- Úselo ListReceiptFilters con un AWS SDK o CLI
- Úselo ListTemplates con un AWS SDK o CLI
- Úselo SendBulkTemplatedEmail con un AWS SDK o CLI
- Úselo SendEmail con un AWS SDK o CLI
- Úselo SendRawEmail con un AWS SDK o CLI
- Úselo SendTemplatedEmail con un AWS SDK o CLI
- Úselo UpdateTemplate con un AWS SDK o CLI
- Úselo VerifyDomainIdentity con un AWS SDK o CLI
- Úselo VerifyEmailIdentity con un AWS SDK o CLI

- Escenarios para Amazon SES con AWS SDK
  - Copie las identidades de correo electrónico y dominio de Amazon SES de una AWS región a otra mediante un AWS SDK
  - Generación de credenciales para conectarse a un punto de conexión SMTP de Amazon SES
  - Verificar la identidad de un correo electrónico y enviar mensajes con Amazon SES mediante un AWS SDK
- Ejemplos de servicios cruzados para Amazon SES que utilizan SDK AWS
  - Creación de una aplicación de streaming de Amazon Transcribe
  - Creación de una aplicación web para hacer un seguimiento de los datos de DynamoDB
  - Crear un rastreador de artículos de Amazon Redshift
  - Crear un rastreador de elementos de trabajo de Aurora Serverless
  - Detecte el PPE en las imágenes con Amazon Rekognition AWS mediante un SDK
  - Detecte objetos en imágenes con Amazon Rekognition AWS mediante un SDK
  - Detecte personas y objetos en un vídeo con Amazon Rekognition AWS mediante un SDK
  - Uso de Step Functions para invocar funciones de Lambda

Acciones para Amazon SES mediante AWS SDK

Los siguientes ejemplos de código muestran cómo realizar acciones individuales de Amazon SES con AWS los SDK. Estos fragmentos llaman a la API de Amazon SES y son fragmentos de código de programas más grandes que se deben ejecutar en contexto. Cada ejemplo incluye un enlace a GitHub, donde puede encontrar instrucciones para configurar y ejecutar el código.

Los siguientes ejemplos incluyen solo las acciones que se utilizan con mayor frecuencia. Para obtener una lista completa, consulte la Referencia de la API de Amazon Simple Email Service (Amazon SES).

Ejemplos

- Úselo CreateReceiptFilter con un AWS SDK o CLI
- Úselo CreateReceiptRule con un AWS SDK o CLI
- Úselo CreateReceiptRuleSet con un AWS SDK o CLI
- Úselo CreateTemplate con un AWS SDK o CLI
- Úselo DeleteIdentity con un AWS SDK o CLI
- Úselo DeleteReceiptFilter con un AWS SDK o CLI
- Úselo DeleteReceiptRule con un AWS SDK o CLI
- Úselo DeleteReceiptRuleSet con un AWS SDK o CLI
- Úselo DeleteTemplate con un AWS SDK o CLI
- Úselo DescribeReceiptRuleSet con un AWS SDK o CLI
- Úselo GetIdentityVerificationAttributes con un AWS SDK o CLI
- Úselo GetSendQuota con un AWS SDK o CLI
- Úselo GetSendStatistics con un AWS SDK o CLI
- Úselo GetTemplate con un AWS SDK o CLI
- Úselo ListIdentities con un AWS SDK o CLI
- Úselo ListReceiptFilters con un AWS SDK o CLI
- Úselo ListTemplates con un AWS SDK o CLI
- Úselo SendBulkTemplatedEmail con un AWS SDK o CLI
- Úselo SendEmail con un AWS SDK o CLI
- Úselo SendRawEmail con un AWS SDK o CLI
- Úselo SendTemplatedEmail con un AWS SDK o CLI

- Úselo UpdateTemplate con un AWS SDK o CLI
- Úselo VerifyDomainIdentity con un AWS SDK o CLI
- Úselo VerifyEmailIdentity con un AWS SDK o CLI

Úselo **`CreateReceiptFilter`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `CreateReceiptFilter`.

C++

SDK para C++

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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();
}
```

- Para obtener más información sobre la API, consulta CreateReceiptFilterla Referencia AWS SDK for C++ de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
  }
};
```

- Para obtener más información sobre la API, consulta CreateReceiptFilterla Referencia AWS SDK for JavaScript de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta CreateReceiptFilterla AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de Amazon SES con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`CreateReceiptRule`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `CreateReceiptRule`.

C++

SDK para C++

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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();
}
```

- Para obtener más información sobre la API, consulta CreateReceiptRulela Referencia AWS SDK for C++ de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
  }
};
```

- Para obtener más información sobre la API, consulta CreateReceiptRulela Referencia AWS SDK for JavaScript de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Cree un bucket de Amazon S3 en el que Amazon SES pueda incluir copias de correos electrónicos entrantes y crear una regla que copie el correo electrónico entrante en el bucket para una lista específica de destinatarios.

```
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
```

- Para obtener más información sobre la API, consulta CreateReceiptRulela AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de Amazon SES con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`CreateReceiptRuleSet`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `CreateReceiptRuleSet`.

C++

SDK para C++

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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();
}
```

- Para obtener más información sobre la API, consulta CreateReceiptRuleSetla Referencia AWS SDK for C++ de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
  }
};
```

- Para obtener más información sobre la API, consulta CreateReceiptRuleSetla Referencia AWS SDK for JavaScript de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta CreateReceiptRuleSetla AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de Amazon SES con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`CreateTemplate`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `CreateTemplate`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Verificación de una identidad de correo electrónico y envío de mensajes

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
    }
```

- Para obtener más información sobre la API, consulta CreateTemplatela Referencia AWS SDK for .NET de la API.

C++

SDK para C++

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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();
}
```

- Para obtener más información sobre la API, consulta CreateTemplatela Referencia AWS SDK for C++ de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
  }
};
```

- Para obtener más información sobre la API, consulta CreateTemplatela Referencia AWS SDK for JavaScript de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta CreateTemplatela AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de Amazon SES con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`DeleteIdentity`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DeleteIdentity`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Verificación de una identidad de correo electrónico y envío de mensajes

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
    }
```

- Para obtener más información sobre la API, consulta DeleteIdentityla Referencia AWS SDK for .NET de la API.

C++

SDK para C++

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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();
}
```

- Para obtener más información sobre la API, consulta DeleteIdentityla Referencia AWS SDK for C++ de la API.

CLI

AWS CLI

Para eliminar una identidad

En el siguiente ejemplo, se utiliza el comando `delete-identity` para eliminar una identidad de la lista de identidades verificadas con Amazon SES:

```
aws ses delete-identity --identity user@example.com
```

Para obtener más información sobre las identidades verificadas, consulte Verificación de direcciones de correo electrónico y dominios en Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener más información sobre la API, consulta DeleteIdentityla Referencia de AWS CLI comandos.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
  }
};
```

- Para obtener más información sobre la API, consulta DeleteIdentityla Referencia AWS SDK for JavaScript de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta DeleteIdentityla AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de Amazon SES con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`DeleteReceiptFilter`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DeleteReceiptFilter`.

C++

SDK para C++

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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();
}
```

- Para obtener más información sobre la API, consulta DeleteReceiptFilterla Referencia AWS SDK for C++ de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
  }
};
```

- Para obtener más información sobre la API, consulta DeleteReceiptFilterla Referencia AWS SDK for JavaScript de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta DeleteReceiptFilterla AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de Amazon SES con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`DeleteReceiptRule`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DeleteReceiptRule`.

C++

SDK para C++

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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();
}
```

- Para obtener más información sobre la API, consulta DeleteReceiptRulela Referencia AWS SDK for C++ de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
  }
};
```

- Para obtener más información sobre la API, consulta DeleteReceiptRulela Referencia AWS SDK for JavaScript de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta DeleteReceiptRulela AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de Amazon SES con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`DeleteReceiptRuleSet`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DeleteReceiptRuleSet`.

C++

SDK para C++

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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();
}
```

- Para obtener más información sobre la API, consulta DeleteReceiptRuleSetla Referencia AWS SDK for C++ de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
  }
};
```

- Para obtener más información sobre la API, consulta DeleteReceiptRuleSetla Referencia AWS SDK for JavaScript de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta DeleteReceiptRuleSetla AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de Amazon SES con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`DeleteTemplate`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DeleteTemplate`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Verificación de una identidad de correo electrónico y envío de mensajes

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
    }
```

- Para obtener más información sobre la API, consulta DeleteTemplatela Referencia AWS SDK for .NET de la API.

C++

SDK para C++

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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();
}
```

- Para obtener más información sobre la API, consulta DeleteTemplatela Referencia AWS SDK for C++ de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
  }
};
```

- Para obtener más información sobre la API, consulta DeleteTemplatela Referencia AWS SDK for JavaScript de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta DeleteTemplatela AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de Amazon SES con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`DescribeReceiptRuleSet`** con un AWS SDK o CLI

En el siguiente ejemplo de código, se muestra cómo usar `DescribeReceiptRuleSet`.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta DescribeReceiptRuleSetla AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de Amazon SES con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`GetIdentityVerificationAttributes`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `GetIdentityVerificationAttributes`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Verificación de una identidad de correo electrónico y envío de mensajes

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
    }
```

- Para obtener más información sobre la API, consulta GetIdentityVerificationAttributesla Referencia AWS SDK for .NET de la API.

CLI

AWS CLI

Para obtener el estado de verificación de Amazon SES de una lista de identidades

En el siguiente ejemplo, se utiliza el comando `get-identity-verification-attributes` para recuperar el estado de verificación de Amazon SES de una lista de identidades:

```
aws ses get-identity-verification-attributes --identities "user1@example.com"
 "user2@example.com"
```

Salida:

```
{
   "VerificationAttributes": {
       "user1@example.com": {
           "VerificationStatus": "Success"
       },
       "user2@example.com": {
           "VerificationStatus": "Pending"
       }
   }
}
```

Si llama a este comando con una identidad que nunca ha enviado para su verificación, esa identidad no aparecerá en el resultado.

Para obtener más información sobre las identidades verificadas, consulte Verificación de direcciones de correo electrónico y dominios en Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener más información sobre la API, consulta GetIdentityVerificationAttributesla Referencia de AWS CLI comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta GetIdentityVerificationAttributesla AWS Referencia de API de SDK for Python (Boto3).

Ruby

SDK para Ruby

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
require "aws-sdk-ses"  # v2: require 'aws-sdk'

# Create client in us-west-2 region
```

```
# Replace us-west-2 with the AWS Region you're using for Amazon SES.
client = Aws::SES::Client.new(region: "us-west-2")

# Get up to 1000 identities
ids = client.list_identities({
  identity_type: "EmailAddress"
})

ids.identities.each do |email|
  attrs = client.get_identity_verification_attributes({
    identities: [email]
  })

  status = attrs.verification_attributes[email].verification_status

  # Display email addresses that have been verified
  if status == "Success"
    puts email
  end
end
```

- Para obtener más información sobre la API, consulta GetIdentityVerificationAttributesla Referencia AWS SDK for Ruby de la API.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`GetSendQuota`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `GetSendQuota`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
    }
```

- Para obtener más información sobre la API, consulta GetSendQuotala Referencia AWS SDK for .NET de la API.

CLI

AWS CLI

Para obtener los límites de envío de Amazon SES

En el siguiente ejemplo, se utiliza el comando `get-send-quota` para devolver los límites de envío de Amazon SES:

```
aws ses get-send-quota
```

Salida:

```
{
```

```
    "Max24HourSend": 200.0,
    "SentLast24Hours": 1.0,
    "MaxSendRate": 1.0
}
```

Max24 HourSend es tu cuota de envío, que es la cantidad máxima de correos electrónicos que puedes enviar en un período de 24 horas. La cuota de envío refleja un período de tiempo acumulativo. Cada vez que intenta enviar un correo electrónico, Amazon SES comprueba la cantidad de correos electrónicos que envió en las 24 horas anteriores. Siempre que el número total de mensajes de correo electrónico que haya enviado sea inferior a su cuota, se aceptará su solicitud de envío y se enviará su correo electrónico.

SentLast24 horas es el número de correos electrónicos que has enviado en las últimas 24 horas.

MaxSendRate es el número máximo de correos electrónicos que puedes enviar por segundo.

Tenga en cuenta que los límites de envío se basan en los destinatarios en lugar de en los mensajes. Por ejemplo, un correo electrónico que tenga 10 destinatarios se contabiliza como 10 en la cuota de envío.

Para obtener más información, consulte Administración de los límites de envío de Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener más información sobre la API, consulta GetSendQuotala Referencia de AWS CLI comandos.

PowerShell

Herramientas para PowerShell

Ejemplo 1: Este comando devuelve los límites de envío actuales del usuario.

```
Get-SESSendQuota
```

- Para obtener más información sobre la API, consulte GetSendQuotala referencia de AWS Tools for PowerShell cmdlets.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de Amazon SES con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`GetSendStatistics`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `GetSendStatistics`.

CLI

AWS CLI

Para obtener tus estadísticas de envíos de Amazon SES

En el siguiente ejemplo, se utiliza el `get-send-statistics` comando para devolver las estadísticas de envío de Amazon SES.

```
aws ses get-send-statistics
```

Salida:

```
{
   "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
       }
   ]
}
```

El resultado es una lista de puntos de datos que representan las dos últimas semanas de actividad de envío. Cada punto de datos de la lista contiene estadísticas para un intervalo de 15 minutos.

En este ejemplo, solo hay dos puntos de datos porque los únicos correos electrónicos que el usuario envió en las últimas dos semanas se produjeron en dos intervalos de 15 minutos.

Para obtener más información, consulte Monitorización de las estadísticas de uso de Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener más información sobre la API, consulte GetSendStatisticsla Referencia de AWS CLI comandos.

PowerShell

Herramientas para PowerShell

Ejemplo 1: Este comando devuelve las estadísticas de envío del usuario. El resultado es una lista de puntos de datos que representan las dos últimas semanas de actividad de envío. Cada punto de datos de la lista contiene estadísticas para un intervalo de 15 minutos.

```
Get-SESSendStatistic
```

- Para obtener más información sobre la API, consulte GetSendStatisticsla referencia de AWS Tools for PowerShell cmdlets.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de Amazon SES con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`GetTemplate`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `GetTemplate`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en su contexto en el siguiente ejemplo de código:

- Verificación de una identidad de correo electrónico y envío de mensajes

C++

SDK para C++

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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();
}
```

- Para obtener más información sobre la API, consulta GetTemplatela Referencia AWS SDK for C++ de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
  }
};
```

- Para obtener más información sobre la API, consulta GetTemplatela Referencia AWS SDK for JavaScript de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta GetTemplatela AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de Amazon SES con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`ListIdentities`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `ListIdentities`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en los siguientes ejemplos de código:

- Copiar identidades de correo electrónico y dominio entre regiones
- Verificación de una identidad de correo electrónico y envío de mensajes

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
    }
```

- Para obtener más información sobre la API, consulta ListIdentitiesla Referencia AWS SDK for .NET de la API.

C++

SDK para C++

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
}
```

- Para obtener más información sobre la API, consulta ListIdentitiesla Referencia AWS SDK for C++ de la API.

CLI

AWS CLI

Para enumerar todas las identidades (direcciones de correo electrónico y dominios) de una AWS cuenta específica

En el siguiente ejemplo, se utiliza el comando `list-identities` para mostrar todas las identidades que se han enviado para su verificación con Amazon SES:

```
aws ses list-identities
```

Salida:

```
{
    "Identities": [
      "user@example.com",
      "example.com"
    ]
```

```
}
```

La lista que se devuelve contiene todas las identidades, independientemente del estado de la verificación (verificada, pendiente de verificación, error, etc.).

En este ejemplo, se devuelven las direcciones de correo electrónico y los dominios porque no especificamos el parámetro de tipo de identidad.

Para obtener más información sobre la verificación, consulte Verificación de direcciones de correo electrónico y dominios en Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener más información sobre la API, consulte ListIdentitiesla Referencia de AWS CLI comandos.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.ses.SesClient;
import software.amazon.awssdk.services.ses.model.ListIdentitiesResponse;
import software.amazon.awssdk.services.ses.model.SesException;
import java.io.IOException;
import java.util.List;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
```

```
public class ListIdentities {

    public static void main(String[] args) throws IOException {
        Region region = Region.US_WEST_2;
        SesClient client = SesClient.builder()
                .region(region)
                .build();

        listSESIdentities(client);
    }

    public static void listSESIdentities(SesClient client) {
        try {
            ListIdentitiesResponse identitiesResponse = client.listIdentities();
            List<String> identities = identitiesResponse.identities();
            for (String identity : identities) {
                System.out.println("The identity is " + identity);
            }

        } catch (SesException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
}
```

- Para obtener más información sobre la API, consulta ListIdentitiesla Referencia AWS SDK for Java 2.x de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
  }
};
```

- Para obtener más información sobre la API, consulta ListIdentitiesla Referencia AWS SDK for JavaScript de la API.

PowerShell

Herramientas para PowerShell

Ejemplo 1: Este comando devuelve una lista que contiene todas las identidades (direcciones de correo electrónico y dominios) de una AWS cuenta específica, independientemente del estado de verificación.

```
Get-SESIdentity
```

- Para obtener más información sobre la API, consulte ListIdentitiesla referencia de AWS Tools for PowerShell cmdlets.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta ListIdentitiesla AWS Referencia de API de SDK for Python (Boto3).

Ruby

SDK para Ruby

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
require "aws-sdk-ses"  # v2: require 'aws-sdk'

# Create client in us-west-2 region
# Replace us-west-2 with the AWS Region you're using for Amazon SES.
client = Aws::SES::Client.new(region: "us-west-2")

# Get up to 1000 identities
ids = client.list_identities({
  identity_type: "EmailAddress"
})

ids.identities.each do |email|
  attrs = client.get_identity_verification_attributes({
    identities: [email]
  })

  status = attrs.verification_attributes[email].verification_status

  # Display email addresses that have been verified
  if status == "Success"
    puts email
  end
end
```

- Para obtener más información sobre la API, consulta ListIdentitiesla Referencia AWS SDK for Ruby de la API.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`ListReceiptFilters`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `ListReceiptFilters`.

C++

SDK para C++

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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();
}
```

- Para obtener más información sobre la API, consulta ListReceiptFiltersla Referencia AWS SDK for C++ de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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);
};
```

- Para obtener más información sobre la API, consulta ListReceiptFiltersla Referencia AWS SDK for JavaScript de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta ListReceiptFilterslа AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de Amazon SES con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`ListTemplates`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `ListTemplates`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Verificación de una identidad de correo electrónico y envío de mensajes

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
    }
```

- Para obtener más información sobre la API, consulta ListTemplatesla Referencia AWS SDK for .NET de la API.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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);
        }
    }
}
```

- Para obtener más información sobre la API, consulta ListTemplatesla Referencia AWS SDK for Java 2.x de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
  }
};
```

- Para obtener más información sobre la API, consulta ListTemplatesla Referencia AWS SDK for JavaScript de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta ListTemplatesla AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de Amazon SES con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`SendBulkTemplatedEmail`** con un AWS SDK o CLI

En el siguiente ejemplo de código, se muestra cómo usar `SendBulkTemplatedEmail`.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
  }
};
```

- Para obtener más información sobre la API, consulta SendBulkTemplatedEmailla Referencia AWS SDK for JavaScript de la API.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`SendEmail`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `SendEmail`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Verificación de una identidad de correo electrónico y envío de mensajes

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
  }
```

- Para obtener más información sobre la API, consulta SendEmailla Referencia AWS SDK for .NET de la API.

C++

SDK para C++

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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();
}
```

- Para obtener más información sobre la API, consulta SendEmailla Referencia AWS SDK for C++ de la API.

CLI

AWS CLI

Para enviar un correo electrónico formateado con Amazon SES

En el siguiente ejemplo, se utiliza el comando `send-email` para enviar un correo electrónico formateado:

```
aws ses send-email --from sender@example.com --destination file://
destination.json --message file://message.json
```

Salida:

```
{
   "MessageId": "EXAMPLEf3a5efcd1-51adec81-d2a4-4e3f-9fe2-5d85c1b23783-000000"
}
```

El destino y el mensaje son estructuras de datos de JSON guardadas en archivos .json en el directorio actual. Estos archivos son los siguientes:

`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"
       }
   }
}
```

Sustituya las direcciones de correo electrónico del remitente y del destinatario por las que desee utilizar. Tenga en cuenta que la dirección de correo electrónico del remitente se debe verificar con Amazon SES. Hasta que se le conceda el acceso de producción a Amazon SES, también debe verificar la dirección de correo electrónico de cada destinatario, a menos que el destinatario sea el simulador de bandeja de correo de Amazon SES. Para obtener más información sobre la verificación, consulte Verificación de direcciones de correo electrónico y dominios en Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

El ID del mensaje en el resultado indica que la llamada para enviar el correo electrónico se ha realizado correctamente.

Si no recibe el correo electrónico, marque la casilla de correo no deseado.

Para obtener más información sobre el envío de correo electrónico formateado, consulte Envío de correo electrónico formateado con la API de Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener más información sobre la API, consulta SendEmailla Referencia de AWS CLI comandos.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.ses.SesClient;
import software.amazon.awssdk.services.ses.model.Content;
import software.amazon.awssdk.services.ses.model.Destination;
import software.amazon.awssdk.services.ses.model.Message;
import software.amazon.awssdk.services.ses.model.Body;
import software.amazon.awssdk.services.ses.model.SendEmailRequest;
import software.amazon.awssdk.services.ses.model.SesException;

import javax.mail.MessagingException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class SendMessageEmailRequest {
    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <sender> <recipient> <subject>\s

                Where:
                    sender - An email address that represents the sender.\s
                    recipient -  An email address that represents the recipient.
\s
                    subject - The  subject line.\s
```

```
                """;

        if (args.length != 3) {
            System.out.println(usage);
            System.exit(1);
        }

        String sender = args[0];
        String recipient = args[1];
        String subject = args[2];

        Region region = Region.US_EAST_1;
        SesClient client = SesClient.builder()
                .region(region)
                .build();

        // The HTML body of the email.
        String bodyHTML = "<html>" + "<head></head>" + "<body>" + "<h1>Hello!</
h1>"
                + "<p> See the list of customers.</p>" + "</body>" + "</html>";

        try {
            send(client, sender, recipient, subject, bodyHTML);
            client.close();
            System.out.println("Done");

        } catch (MessagingException e) {
            e.getStackTrace();
        }
    }

    public static void send(SesClient client,
            String sender,
            String recipient,
            String subject,
            String bodyHTML) throws MessagingException {

        Destination destination = Destination.builder()
                .toAddresses(recipient)
                .build();

        Content content = Content.builder()
                .data(bodyHTML)
                .build();
```

```
        Content sub = Content.builder()
                .data(subject)
                .build();

        Body body = Body.builder()
                .html(content)
                .build();

        Message msg = Message.builder()
                .subject(sub)
                .body(body)
                .build();

        SendEmailRequest emailRequest = SendEmailRequest.builder()
                .destination(destination)
                .message(msg)
                .source(sender)
                .build();

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

        } catch (SesException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
}

import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.ses.SesClient;
import javax.activation.DataHandler;
import javax.activation.DataSource;
import javax.mail.Message;
import javax.mail.MessagingException;
import javax.mail.Session;
import javax.mail.internet.AddressException;
import javax.mail.internet.InternetAddress;
import javax.mail.internet.MimeMessage;
import javax.mail.internet.MimeMultipart;
import javax.mail.internet.MimeBodyPart;
```

```
import javax.mail.util.ByteArrayDataSource;
import java.io.ByteArrayOutputStream;
import java.io.IOException;
import java.nio.ByteBuffer;
import java.nio.file.Files;
import java.util.Properties;
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.services.ses.model.SendRawEmailRequest;
import software.amazon.awssdk.services.ses.model.RawMessage;
import software.amazon.awssdk.services.ses.model.SesException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class SendMessageAttachment {
    public static void main(String[] args) throws IOException {
        final String usage = """

                Usage:
                    <sender> <recipient> <subject> <fileLocation>\s

                Where:
                    sender - An email address that represents the sender.\s
                    recipient -  An email address that represents the recipient.
\s
                    subject - The  subject line.\s
                    fileLocation - The location of a Microsoft Excel file to use
 as an attachment (C:/AWS/customers.xls).\s
                """;

        if (args.length != 4) {
            System.out.println(usage);
            System.exit(1);
        }

        String sender = args[0];
        String recipient = args[1];
```

```
        String subject = args[2];
        String fileLocation = args[3];

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

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

        Region region = Region.US_WEST_2;
        SesClient client = SesClient.builder()
                .region(region)
                .build();

        try {
            sendemailAttachment(client, sender, recipient, subject, bodyText,
 bodyHTML, fileLocation);
            client.close();
            System.out.println("Done");

        } catch (IOException | MessagingException e) {
            e.getStackTrace();
        }
    }

    public static void sendemailAttachment(SesClient client,
            String sender,
            String recipient,
            String subject,
            String bodyText,
            String bodyHTML,
            String fileLocation) throws AddressException, MessagingException,
 IOException {

        java.io.File theFile = new java.io.File(fileLocation);
        byte[] fileContent = Files.readAllBytes(theFile.toPath());

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

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

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

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

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

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

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

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

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

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

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

        // Define the attachment.
        MimeBodyPart att = new MimeBodyPart();
        DataSource fds = new ByteArrayDataSource(fileContent,
                "application/vnd.openxmlformats-
officedocument.spreadsheetml.sheet");
        att.setDataHandler(new DataHandler(fds));
```

```
        String reportName = "WorkReport.xls";
        att.setFileName(reportName);

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

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

            ByteArrayOutputStream outputStream = new ByteArrayOutputStream();
            message.writeTo(outputStream);

            ByteBuffer buf = ByteBuffer.wrap(outputStream.toByteArray());

            byte[] arr = new byte[buf.remaining()];
            buf.get(arr);

            SdkBytes data = SdkBytes.fromByteArray(arr);
            RawMessage rawMessage = RawMessage.builder()
                    .data(data)
                    .build();

            SendRawEmailRequest rawEmailRequest = SendRawEmailRequest.builder()
                    .rawMessage(rawMessage)
                    .build();

            client.sendRawEmail(rawEmailRequest);

        } catch (SesException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        System.out.println("Email sent using SesClient with attachment");
    }
}
```

- Para obtener más información sobre la API, consulta SendEmailla Referencia AWS SDK for Java 2.x de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
  }
};
```

- Para obtener más información sobre la API, consulta SendEmailla Referencia AWS SDK for JavaScript de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta SendEmailla AWS Referencia de API de SDK for Python (Boto3).

Ruby

SDK para Ruby

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
require "aws-sdk-ses"  # v2: require 'aws-sdk'

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

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

# Specify a configuration set. To use a configuration
# set, uncomment the next line and line 74.
#   configsetname = "ConfigSet"
```

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

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

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

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

# Create a new SES client in the us-west-2 region.
# Replace us-west-2 with the AWS Region you're using for Amazon SES.
ses = Aws::SES::Client.new(region: "us-west-2")

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

```
    },
    source: sender,
    # Uncomment the following line to use a configuration set.
    # configuration_set_name: configsetname,
    )

  puts "Email sent to " + recipient

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

- Para obtener más información sobre la API, consulta SendEmailla Referencia AWS SDK for Ruby de la API.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`SendRawEmail`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `SendRawEmail`.

CLI

AWS CLI

Para enviar un correo electrónico sin procesar con Amazon SES

En el siguiente ejemplo, se utiliza el comando `send-raw-email` para enviar un correo electrónico con un TXT adjunto:

```
aws ses send-raw-email --raw-message file://message.json
```

Salida:

```
{
   "MessageId": "EXAMPLEf3f73d99b-c63fb06f-d263-41f8-a0fb-d0dc67d56c07-000000"
```

```
}
```

El mensaje sin procesar es una estructura de datos JSON guardada en un archivo denominado `message.json` en el directorio actual. Contiene lo siguiente:

```
{
   "Data": "From: sender@example.com\nTo: recipient@example.com\nSubject:
 Test email sent using the AWS CLI (contains an attachment)\nMIME-Version:
 1.0\nContent-type: Multipart/Mixed; boundary=\"NextPart\"\n\n--NextPart
\nContent-Type: text/plain\n\nThis is the message body.\n\n--NextPart\nContent-
Type: text/plain;\nContent-Disposition: attachment; filename=\"attachment.txt\"\n
\nThis is the text in the attachment.\n\n--NextPart--"
}
```

Como puede ver, “Datos” es una cadena larga que contiene todo el contenido sin procesar del correo electrónico en formato MIME, incluido un archivo adjunto llamado attachment.txt.

Sustituya sender@example.com y recipient@example.com por las direcciones que desee utilizar. Tenga en cuenta que la dirección de correo electrónico del remitente se debe verificar con Amazon SES. Hasta que se le conceda el acceso de producción a Amazon SES, también debe verificar la dirección de correo electrónico del destinatario, a menos que el destinatario sea el simulador de bandeja de correo de Amazon SES. Para obtener más información sobre la verificación, consulte Verificación de direcciones de correo electrónico y dominios en Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

El identificador del mensaje en el resultado indica que la llamada a send-raw-email se realizó correctamente.

Si no recibe el correo electrónico, marque la casilla de correo no deseado.

Para obtener más información sobre el envío de correo electrónico sin procesar, consulte Envío de correo electrónico sin procesar con la API de Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener más información sobre la API, consulte SendRawEmailla Referencia de AWS CLI comandos.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Utilice nodemailer para enviar un correo electrónico con un archivo adjunto.

```
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);
        }
      },
    );
  });
};
```

- Para obtener más información sobre la API, consulta SendRawEmailla Referencia AWS SDK for JavaScript de la API.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`SendTemplatedEmail`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `SendTemplatedEmail`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Verificación de una identidad de correo electrónico y envío de mensajes

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
   }
```

- Para obtener más información sobre la API, consulta SendTemplatedEmailla Referencia AWS SDK for .NET de la API.

C++

SDK para C++

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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::SendTtemplatedEmailRequest 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();
}
```

- Para obtener más información sobre la API, consulta SendTemplatedEmailla Referencia AWS SDK for C++ de la API.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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);
        }
    }
}
```

- Para obtener más información sobre la API, consulta SendTemplatedEmailla Referencia AWS SDK for Java 2.x de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
  }
};
```

- Para obtener más información sobre la API, consulta SendTemplatedEmailla Referencia AWS SDK for JavaScript de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta SendTemplatedEmailla AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de Amazon SES con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`UpdateTemplate`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `UpdateTemplate`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en su contexto en el siguiente ejemplo de código:

- Verificación de una identidad de correo electrónico y envío de mensajes

C++

SDK para C++

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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();
}
```

- Para obtener más información sobre la API, consulta UpdateTemplatela Referencia AWS SDK for C++ de la API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
  }
};
```

- Para obtener más información sobre la API, consulta UpdateTemplatela Referencia AWS SDK for JavaScript de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta UpdateTemplatela AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de Amazon SES con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`VerifyDomainIdentity`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `VerifyDomainIdentity`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en los siguientes ejemplos de código:

- Copiar identidades de correo electrónico y dominio entre regiones
- Verificación de una identidad de correo electrónico y envío de mensajes

CLI

AWS CLI

Para verificar un dominio con Amazon SES

En el siguiente ejemplo, se usa el comando `verify-domain-identity` para verificar un dominio:

```
aws ses verify-domain-identity --domain example.com
```

Salida:

```
{
   "VerificationToken": "eoEmxw+YaYhb3h3iVJHuXMJXqeu1q1/wwmvjuEXAMPLE"
}
```

Para completar la verificación del dominio, debe agregar un registro TXT con el token de verificación devuelto a la configuración de DNS del dominio. Para obtener más información, consulte Verificación de dominios en Amazon SES en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener más información sobre la API, consulte VerifyDomainIdentityla Referencia de AWS CLI comandos.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
  }
};
```

- Para obtener más información sobre la API, consulta VerifyDomainIdentityla Referencia AWS SDK for JavaScript de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta VerifyDomainIdentityla AWS Referencia de API de SDK for Python (Boto3).

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulte. Uso de Amazon SES con un AWS SDK En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`VerifyEmailIdentity`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `VerifyEmailIdentity`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en los siguientes ejemplos de código:

- Copiar identidades de correo electrónico y dominio entre regiones

- Verificación de una identidad de correo electrónico y envío de mensajes

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
```

```
    }
```

- Para obtener más información sobre la API, consulta VerifyEmailIdentityla Referencia AWS SDK for .NET de la API.

C++

SDK para C++

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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();
}
```

- Para obtener más información sobre la API, consulta VerifyEmailIdentityla Referencia AWS SDK for C++ de la API.

CLI

AWS CLI

Para verificar una dirección de correo electrónico con Amazon SES

En el siguiente ejemplo, se usa el comando `verify-email-identity` para verificar una dirección de correo electrónico:

```
aws ses verify-email-identity --email-address user@example.com
```

Antes de poder enviar un correo electrónico mediante Amazon SES, debe verificar la dirección o el dominio desde el que envía el correo electrónico para demostrar que es de su propiedad. Si todavía no tiene acceso de producción, también deberá verificar las direcciones de correo electrónico a las que envíe correos electrónicos, excepto las proporcionadas por el simulador de buzón de correo de Amazon SES.

Cuando verify-email-identity se llame, la dirección de correo electrónico recibirá un correo electrónico de verificación. El usuario debe hacer clic en el enlace del correo electrónico para completar el proceso de verificación.

Para obtener más información, consulte Verificación de direcciones de correo electrónico en Amazon SES, en la Guía para desarrolladores de Amazon Simple Email Service.

- Para obtener más información sobre la API, consulte VerifyEmailIdentityla Referencia de AWS CLI comandos.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
  }
};
```

- Para obtener más información sobre la API, consulta VerifyEmailIdentityla Referencia AWS SDK for JavaScript de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta VerifyEmailIdentityla AWS Referencia de API de SDK for Python (Boto3).

Ruby

SDK para Ruby

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
require "aws-sdk-ses"  # v2: require 'aws-sdk'

# Replace recipient@example.com with a "To" address.
recipient = "recipient@example.com"

# Create a new SES resource in the us-west-2 region.
# Replace us-west-2 with the AWS Region you're using for Amazon SES.
ses = Aws::SES::Client.new(region: "us-west-2")

# Try to verify email address.
begin
  ses.verify_email_identity({
    email_address: recipient
  })

  puts "Email sent to " + recipient

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

- Para obtener más información sobre la API, consulta VerifyEmailIdentityla Referencia AWS SDK for Ruby de la API.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Escenarios para Amazon SES con AWS SDK

Los siguientes ejemplos de código muestran cómo implementar escenarios comunes en Amazon SES con AWS SDK. Estos escenarios muestran cómo llevar a cabo tareas específicas llamando a varias funciones dentro de Amazon SES. Cada escenario incluye un enlace a GitHub, donde puede encontrar instrucciones sobre cómo configurar y ejecutar el código.

Ejemplos

- Copie las identidades de correo electrónico y dominio de Amazon SES de una AWS región a otra mediante un AWS SDK
- Generación de credenciales para conectarse a un punto de conexión SMTP de Amazon SES
- Verificar la identidad de un correo electrónico y enviar mensajes con Amazon SES mediante un AWS SDK

Copie las identidades de correo electrónico y dominio de Amazon SES de una AWS región a otra mediante un AWS SDK

El siguiente ejemplo de código muestra cómo copiar las identidades de correo electrónico y dominio de Amazon SES de una AWS región a otra. Cuando Route 53 administra las identidades de dominio, los registros de verificación se copian en el dominio de la región de destino.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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()
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de la API de AWS SDK para Python (Boto3).
  - ListIdentities
  - SetIdentityNotificationTopic
  - VerifyDomainDkim
  - VerifyDomainIdentity
  - VerifyEmailIdentity

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Generación de credenciales para conectarse a un punto de conexión SMTP de Amazon SES

El siguiente ejemplo de código muestra cómo generar credenciales para conectarse a un punto de conexión SMTP de Amazon SES.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

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

import hmac
import hashlib
import base64
import argparse

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

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

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


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

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


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


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

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Verificar la identidad de un correo electrónico y enviar mensajes con Amazon SES mediante un AWS SDK

En el siguiente ejemplo de código, se muestra cómo:

- Agregar y verificar una dirección de correo electrónico con Amazon SES.
- Envía un mensaje de correo electrónico estándar.
- Crear una plantilla y enviar un mensaje de correo electrónico con plantilla.
- Enviar un mensaje mediante un servidor SMTP de Amazon SES.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Verifique una dirección de correo electrónico con Amazon SES y envíe mensajes.

```
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)
```

Cree funciones para encapsular acciones de identidad de 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
```

Cree funciones para encapsular acciones de plantillas de 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
```

Cree funciones para encapsular acciones por correo electrónico de 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
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de la API de AWS SDK para Python (Boto3).
  - CreateTemplate
  - DeleteIdentity
  - DeleteTemplate
  - GetIdentityVerificationAttributes
  - GetTemplate
  - ListIdentities
  - ListTemplates
  - SendEmail
  - SendTemplatedEmail
  - UpdateTemplate
  - VerifyDomainIdentity
  - VerifyEmailIdentity

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Ejemplos de servicios cruzados para Amazon SES que utilizan SDK AWS

Los siguientes ejemplos de aplicaciones utilizan AWS SDK para combinar Amazon SES con otros Servicios de AWS. Cada ejemplo incluye un enlace a GitHub, donde puede encontrar instrucciones sobre cómo configurar y ejecutar la aplicación.

Ejemplos

- Creación de una aplicación de streaming de Amazon Transcribe
- Creación de una aplicación web para hacer un seguimiento de los datos de DynamoDB
- Crear un rastreador de artículos de Amazon Redshift
- Crear un rastreador de elementos de trabajo de Aurora Serverless
- Detecte el PPE en las imágenes con Amazon Rekognition AWS mediante un SDK
- Detecte objetos en imágenes con Amazon Rekognition AWS mediante un SDK
- Detecte personas y objetos en un vídeo con Amazon Rekognition AWS mediante un SDK
- Uso de Step Functions para invocar funciones de Lambda

Creación de una aplicación de streaming de Amazon Transcribe

El siguiente ejemplo de código muestra cómo crear una aplicación que grabe, transcriba y traduzca audio en directo en tiempo real para luego enviar por correo electrónico los resultados.

JavaScript

SDK para JavaScript (v3)

Muestra cómo utilizar Amazon Transcribe para crear una aplicación que grabe, transcriba y traduzca audio en directo en tiempo real para luego enviar los resultados por correo electrónico mediante Amazon Simple Email Service (Amazon SES).

Para ver el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulta el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Amazon Comprehend
- Amazon SES
- Amazon Transcribe
- Amazon Translate

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Creación de una aplicación web para hacer un seguimiento de los datos de DynamoDB

Los siguientes ejemplos de código muestran cómo crear una aplicación web que realice un seguimiento de los elementos de trabajo de una tabla de Amazon DynamoDB y use Amazon Simple Email Service (Amazon SES) para enviar informes.

.NET

AWS SDK for .NET

Muestra cómo utilizar la API de .NET de Amazon DynamoDB para crear una aplicación web dinámica que haga un seguimiento de los datos de trabajo de DynamoDB.

Para ver el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulta el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- DynamoDB
- Amazon SES

Java

SDK para Java 2.x

Muestra cómo utilizar la API de Amazon DynamoDB para crear una aplicación web dinámica que haga un seguimiento de los datos de trabajo de DynamoDB.

Para ver el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulta el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- DynamoDB
- Amazon SES

JavaScript

SDK para JavaScript (v3)

Muestra cómo utilizar la API de Amazon DynamoDB para crear una aplicación web dinámica que haga un seguimiento de los datos de trabajo de DynamoDB.

Para ver el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulta el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- DynamoDB
- Amazon SES

Kotlin

SDK para Kotlin

Muestra cómo utilizar la API de Amazon DynamoDB para crear una aplicación web dinámica que haga un seguimiento de los datos de trabajo de DynamoDB.

Para ver el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulta el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- DynamoDB
- Amazon SES

Python

SDK para Python (Boto3)

Muestra cómo usarlo AWS SDK for Python (Boto3) para crear un servicio REST que haga un seguimiento de los elementos de trabajo en Amazon DynamoDB y envíe informes por correo electrónico mediante Amazon Simple Email Service (Amazon SES). En este ejemplo se utiliza el marco web de Flask para gestionar el enrutamiento HTTP y se integra con una página web de React para presentar una aplicación web completamente funcional.

- Cree un servicio REST de Flask que se integre con. Servicios de AWS
- Lea, escriba y actualice los elementos de trabajo almacenados en una tabla de DynamoDB.
- Utilice Amazon SES para enviar informes de elementos de trabajo por correo electrónico.

Para obtener el código fuente completo e instrucciones sobre cómo configurarlo y ejecutarlo, consulte el ejemplo completo en el repositorio de ejemplos de AWS código en GitHub.

Servicios utilizados en este ejemplo

- DynamoDB
- Amazon SES

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Crear un rastreador de artículos de Amazon Redshift

Los siguientes ejemplos de código muestran cómo crear una aplicación web que realice un seguimiento de los elementos de trabajo e informe al respecto con una base de datos de Amazon Redshift.

Java

SDK para Java 2.x

Muestra cómo crear una aplicación web que realice un seguimiento de los elementos de trabajo almacenados en una base de datos de Amazon Redshift e informe al respecto.

Para obtener el código fuente completo y las instrucciones sobre cómo configurar una API REST de Spring que consulte los datos de Amazon Redshift y para que la utilice una aplicación de React, consulte el ejemplo completo en. GitHub

Servicios utilizados en este ejemplo

- Amazon Redshift
- Amazon SES

Kotlin

SDK para Kotlin

Muestra cómo crear una aplicación web que realice un seguimiento de los elementos de trabajo almacenados en una base de datos de Amazon Redshift e informe al respecto.

Para obtener el código fuente completo y las instrucciones sobre cómo configurar una API REST de Spring que consulte los datos de Amazon Redshift y para que la utilice una aplicación de React, consulte el ejemplo completo en. GitHub

Servicios utilizados en este ejemplo

- Amazon Redshift
- Amazon SES

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Crear un rastreador de elementos de trabajo de Aurora Serverless

Los siguientes ejemplos de código muestran cómo crear una aplicación web que realice un seguimiento de los elementos de trabajo de una base de datos de Amazon Aurora sin servidor y use Amazon Simple Email Service (Amazon SES) para enviar informes.

.NET

AWS SDK for .NET

Muestra cómo usarlo AWS SDK for .NET para crear una aplicación web que rastrea los elementos de trabajo en una base de datos de Amazon Aurora y envía informes por correo electrónico mediante Amazon Simple Email Service (Amazon SES). Este ejemplo usa un frontend creado con React.js para interactuar con un backend .NET RESTful.

- Integre una aplicación web de React con AWS los servicios.
- Muestre, agregue, actualice y elimine elementos en una tabla de Aurora.
- Envíe un informe por correo electrónico de elementos de trabajo filtrados con Amazon SES.
- Implemente y gestione recursos de ejemplo con el AWS CloudFormation script incluido.

Para obtener el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulte el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Aurora
- Amazon RDS
- Servicio de datos de Amazon RDS
- Amazon SES

C++

SDK para C++

Muestra cómo crear una aplicación web que realice un seguimiento de los elementos de trabajo almacenados en una base de datos de Amazon Aurora sin servidor e informe al respecto.

Para obtener el código fuente completo y las instrucciones sobre cómo configurar una API REST de C++ que consulte los datos de Amazon Aurora Serverless y para que la utilice una aplicación de React, consulte el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Aurora
- Amazon RDS
- Servicio de datos de Amazon RDS
- Amazon SES

Java

SDK para Java 2.x

Muestra cómo crear una aplicación web que haga un seguimiento de los elementos de trabajo almacenados en una base de datos de Amazon RDS e informe al respecto.

Para obtener el código fuente completo y las instrucciones sobre cómo configurar una API REST de Spring que consulte los datos de Amazon Aurora Serverless y para que la utilice una aplicación React, consulte el ejemplo completo en GitHub.

Para obtener el código fuente completo y las instrucciones sobre cómo configurar y ejecutar un ejemplo que utilice la API JDBC, consulte el ejemplo completo en. GitHub

Servicios utilizados en este ejemplo

- Aurora
- Amazon RDS
- Servicio de datos de Amazon RDS
- Amazon SES

JavaScript

SDK para JavaScript (v3)

Muestra cómo usar la AWS SDK for JavaScript (v3) para crear una aplicación web que rastrea los elementos de trabajo en una base de datos de Amazon Aurora y envía informes por correo electrónico mediante Amazon Simple Email Service (Amazon SES). Este ejemplo usa un frontend creado con React.js para interactuar con un backend de Node.js de Express.

- Integre una aplicación web React.js con Servicios de AWS.
- Cree una lista, agregue y actualice elementos en una tabla de Aurora.
- Envíe un informe por correo electrónico de elementos de trabajo filtrados con Amazon SES.
- Implemente y gestione recursos de ejemplo con el AWS CloudFormation script incluido.

Para obtener el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulte el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Aurora
- Amazon RDS
- Servicio de datos de Amazon RDS
- Amazon SES

Kotlin

SDK para Kotlin

Muestra cómo crear una aplicación web que haga un seguimiento de los elementos de trabajo almacenados en una base de datos de Amazon RDS e informe al respecto.

Para obtener el código fuente completo y las instrucciones sobre cómo configurar una API REST de Spring que consulte los datos de Amazon Aurora Serverless y para que la utilice una aplicación React, consulte el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Aurora
- Amazon RDS
- Servicio de datos de Amazon RDS
- Amazon SES

PHP

SDK para PHP

Muestra cómo utilizarla AWS SDK for PHP para crear una aplicación web que haga un seguimiento de los elementos de trabajo de una base de datos de Amazon RDS y envíe informes por correo electrónico mediante Amazon Simple Email Service (Amazon SES). Este ejemplo usa un front-end creado con React.js para interactuar con un backend PHP RESTful.

- Integre una aplicación web de React.js con AWS los servicios.
- Enumere, agregue, actualice y elimine elementos de una tabla de Amazon RDS.
- Envíe un informe por correo electrónico de elementos de trabajo filtrados con Amazon SES.
- Implemente y gestione recursos de ejemplo con el AWS CloudFormation script incluido.

Para obtener el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulte el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Aurora
- Amazon RDS

- Servicio de datos de Amazon RDS
- Amazon SES

Python

SDK para Python (Boto3)

Muestra cómo usarlo AWS SDK for Python (Boto3) para crear un servicio REST que rastrea los elementos de trabajo en una base de datos Amazon Aurora Serverless y envía informes por correo electrónico mediante Amazon Simple Email Service (Amazon SES). En este ejemplo se utiliza el marco web de Flask para gestionar el enrutamiento HTTP y se integra con una página web de React para presentar una aplicación web completamente funcional.

- Cree un servicio REST de Flask que se integre con. Servicios de AWS
- Lea, escriba y actualice los elementos de trabajo almacenados en una base de datos de Aurora Serverless.
- Cree un AWS Secrets Manager secreto que contenga las credenciales de la base de datos y utilícelo para autenticar las llamadas a la base de datos.
- Utilice Amazon SES para enviar informes de elementos de trabajo por correo electrónico.

Para obtener el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulte el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Aurora
- Amazon RDS
- Servicio de datos de Amazon RDS
- Amazon SES

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Detecte el PPE en las imágenes con Amazon Rekognition AWS mediante un SDK

Los siguientes ejemplos de código muestran cómo crear una aplicación que utiliza Amazon Rekognition para detectar equipos de protección individual (EPI) en imágenes.

Java

SDK para Java 2.x

Muestra cómo crear una AWS Lambda función que detecte imágenes con un equipo de protección individual.

Para obtener el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulte el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- DynamoDB
- Amazon Rekognition
- Amazon S3
- Amazon SES

JavaScript

SDK para JavaScript (v3)

Muestra cómo utilizar Amazon Rekognition AWS SDK for JavaScript con el para crear una aplicación que detecte el equipo de protección personal (EPP) en imágenes ubicadas en un depósito de Amazon Simple Storage Service (Amazon S3). La aplicación guarda los resultados en una tabla de Amazon DynamoDB y envía al administrador una notificación por correo electrónico con los resultados mediante Amazon Simple Email Service (Amazon SES).

Aprenda cómo:

- Crear un usuario no autenticado con Amazon Cognito.
- Analizar imágenes en busca de EPI con Amazon Rekognition.
- Verificar una dirección de correo electrónico de Amazon SES.
- Actualizar una tabla de DynamoDB con resultados.
- Enviar una notificación por correo electrónico con Amazon SES.

Para obtener el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulte el ejemplo completo en. GitHub

Servicios utilizados en este ejemplo

- DynamoDB

- Amazon Rekognition
- Amazon S3
- Amazon SES

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Detecte objetos en imágenes con Amazon Rekognition AWS mediante un SDK

Los siguientes ejemplos de código muestran cómo crear una aplicación que utilice Amazon Rekognition para detectar objetos por categoría en imágenes.

.NET

AWS SDK for .NET

Muestra cómo utilizar la API de .NET de Amazon Rekognition para crear una aplicación que utilice Amazon Rekognition para identificar objetos por categoría en imágenes ubicadas en un bucket de Amazon Simple Storage Service (Amazon S3). La aplicación envía al administrador una notificación por correo electrónico con los resultados mediante Amazon Simple Email Service (Amazon SES).

Para ver el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulta el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Amazon Rekognition
- Amazon S3
- Amazon SES

Java

SDK para Java 2.x

Muestra cómo utilizar la API de Java de Amazon Rekognition para crear una aplicación que utilice Amazon Rekognition para identificar objetos por categoría en imágenes ubicadas en un

bucket de Amazon Simple Storage Service (Amazon S3). La aplicación envía al administrador una notificación por correo electrónico con los resultados mediante Amazon Simple Email Service (Amazon SES).

Para ver el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulta el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Amazon Rekognition
- Amazon S3
- Amazon SES

JavaScript

SDK para JavaScript (v3)

Muestra cómo utilizar Amazon Rekognition AWS SDK for JavaScript con el para crear una aplicación que utilice Amazon Rekognition para identificar objetos por categoría en imágenes ubicadas en un bucket de Amazon Simple Storage Service (Amazon S3). La aplicación envía al administrador una notificación por correo electrónico con los resultados mediante Amazon Simple Email Service (Amazon SES).

Aprenda cómo:

- Crear un usuario no autenticado con Amazon Cognito.
- Analizar imágenes en busca de objetos con Amazon Rekognition.
- Verificar una dirección de correo electrónico de Amazon SES.
- Enviar una notificación por correo electrónico con Amazon SES.

Para obtener el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulte el ejemplo completo en. GitHub

Servicios utilizados en este ejemplo

- Amazon Rekognition
- Amazon S3
- Amazon SES

Kotlin

SDK para Kotlin

Muestra cómo utilizar la API de Kotlin de Amazon Rekognition para crear una aplicación que utilice Amazon Rekognition para identificar objetos por categoría en imágenes ubicadas en un bucket de Amazon Simple Storage Service (Amazon S3). La aplicación envía al administrador una notificación por correo electrónico con los resultados mediante Amazon Simple Email Service (Amazon SES).

Para ver el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulta el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Amazon Rekognition
- Amazon S3
- Amazon SES

Python

SDK para Python (Boto3)

Le muestra cómo utilizar el AWS SDK for Python (Boto3) para crear una aplicación web que le permita hacer lo siguiente:

- Subir fotos en un bucket de Amazon Simple Storage Service (Amazon S3).
- Utilizar Amazon Rekognition para analizar y etiquetar las fotos.
- Utilice Amazon Simple Email Service (Amazon SES) para enviar informes de análisis de imágenes por correo electrónico.

Este ejemplo contiene dos componentes principales: una página web escrita con React y un servicio REST escrito en Python creado con Flask-RESTful. JavaScript

Puede utilizar la página web de React para:

- Mostrar una lista de imágenes almacenadas en el bucket de S3.
- Subir imágenes desde la computadora en el bucket de S3.
- Mostrar imágenes y etiquetas que identifican los elementos detectados en la imagen.

- Obtener un informe de todas las imágenes del bucket de S3 y enviar un correo electrónico del informe.

La página web llama al servicio REST. El servicio envía solicitudes a AWS para llevar a cabo las siguientes acciones:

- Obtener y filtrar la lista de imágenes del bucket de S3.
- Subir fotos en el bucket de S3.
- Utilizar Amazon Rekognition para analizar fotos individuales y obtener una lista de etiquetas que identifican los elementos detectados en la foto.
- Analizar todas las fotos del bucket de S3 y usar Amazon SES para enviar un informe por correo electrónico.

Para ver el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulta el ejemplo completo en. GitHub

Servicios utilizados en este ejemplo

- Amazon Rekognition
- Amazon S3
- Amazon SES

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Detecte personas y objetos en un vídeo con Amazon Rekognition AWS mediante un SDK

Los siguientes ejemplos de código indican cómo detectar personas y objetos en un video con Amazon Rekognition.

Java

SDK para Java 2.x

Muestra cómo utilizar la API Java de Amazon Rekognition para crear una aplicación que detecte rostros y objetos en vídeos ubicados en un bucket de Amazon Simple Storage Service

(Amazon S3). La aplicación envía al administrador una notificación por correo electrónico con los resultados mediante Amazon Simple Email Service (Amazon SES).

Para ver el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulta el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- Amazon Rekognition
- Amazon S3
- Amazon SES

JavaScript

SDK para JavaScript (v3)

Muestra cómo usar Amazon Rekognition AWS SDK for JavaScript con el para crear una aplicación que detecte rostros y objetos en vídeos ubicados en un bucket de Amazon Simple Storage Service (Amazon S3). La aplicación envía al administrador una notificación por correo electrónico con los resultados mediante Amazon Simple Email Service (Amazon SES).

Aprenda cómo:

- Crear un usuario no autenticado con Amazon Cognito.
- Analizar imágenes en busca de EPI con Amazon Rekognition.
- Verificar una dirección de correo electrónico de Amazon SES.
- Enviar una notificación por correo electrónico con Amazon SES.

Para obtener el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulte el ejemplo completo en. GitHub

Servicios utilizados en este ejemplo

- Amazon Rekognition
- Amazon S3
- Amazon SES

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Uso de Step Functions para invocar funciones de Lambda

Los siguientes ejemplos de código muestran cómo crear una máquina de AWS Step Functions estados que invoque AWS Lambda funciones en secuencia.

Java

SDK para Java 2.x

Muestra cómo crear un flujo de trabajo AWS sin servidor mediante AWS Step Functions y el AWS SDK for Java 2.x. Cada paso del flujo de trabajo se implementa mediante una AWS Lambda función.

Para obtener el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulte el ejemplo completo en GitHub.

Servicios utilizados en este ejemplo

- DynamoDB
- Lambda
- Amazon SES
- Step Functions

JavaScript

SDK para JavaScript (v3)

Muestra cómo crear un flujo de trabajo AWS sin servidor mediante AWS Step Functions y el. AWS SDK for JavaScript Cada paso del flujo de trabajo se implementa mediante una AWS Lambda función.

Lambda es un servicio de computación que permite ejecutar código sin aprovisionar ni administrar servidores. Step Functions es un servicio de orquestación sin servidor que le permite combinar funciones de Lambda y otros servicios de AWS para crear aplicaciones esenciales desde el punto de vista empresarial.

Para obtener el código fuente completo y las instrucciones sobre cómo configurarlo y ejecutarlo, consulte el ejemplo completo en GitHub.

Este ejemplo también está disponible en la guía para desarrolladores de AWS SDK for JavaScript v3.

Servicios utilizados en este ejemplo

- DynamoDB
- Lambda
- Amazon SES
- Step Functions

Para obtener una lista completa de las guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Ejemplos de código para la API v2 de Amazon SES con AWS SDK

Los siguientes ejemplos de código muestran cómo utilizar la API v2 de Amazon SES con un kit de desarrollo de AWS software (SDK).

Las acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Mientras las acciones muestran cómo llamar a las funciones de servicio individuales, es posible ver las acciones en contexto en los escenarios relacionados y en los ejemplos entre servicios.

Los escenarios son ejemplos de código que muestran cómo llevar a cabo una tarea específica llamando a varias funciones dentro del mismo servicio.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Ejemplos de código

- Acciones para la API v2 de Amazon SES mediante AWS SDK
  - Úselo CreateContact con un AWS SDK o CLI
  - Úselo CreateContactList con un AWS SDK o CLI
  - Úselo CreateEmailIdentity con un AWS SDK o CLI
  - Úselo CreateEmailTemplate con un AWS SDK o CLI
  - Úselo DeleteContactList con un AWS SDK o CLI
  - Úselo DeleteEmailIdentity con un AWS SDK o CLI

- Úselo DeleteEmailTemplate con un AWS SDK o CLI
- Úselo GetEmailIdentity con un AWS SDK o CLI
- Úselo ListContactLists con un AWS SDK o CLI
- Úselo ListContacts con un AWS SDK o CLI
- Úselo SendEmail con un AWS SDK o CLI

- Escenarios para la API v2 de Amazon SES con AWS SDK
  - Un flujo de trabajo completo para el boletín de Amazon SES API v2 mediante un AWS SDK

Acciones para la API v2 de Amazon SES mediante AWS SDK

Los siguientes ejemplos de código muestran cómo realizar acciones individuales de la API de Amazon SES v2 con AWS los SDK. Estos fragmentos llaman a la API v2 de Amazon SES y son fragmentos de código de programas más grandes que se deben ejecutar en contexto. Cada ejemplo incluye un enlace a GitHub, donde puede encontrar instrucciones para configurar y ejecutar el código.

Los siguientes ejemplos incluyen solo las acciones que se utilizan con mayor frecuencia. Para obtener una lista completa, consulte la Referencia de la API de la API v2 de Amazon Simple Email Service.

Ejemplos

- Úselo CreateContact con un AWS SDK o CLI
- Úselo CreateContactList con un AWS SDK o CLI
- Úselo CreateEmailIdentity con un AWS SDK o CLI
- Úselo CreateEmailTemplate con un AWS SDK o CLI
- Úselo DeleteContactList con un AWS SDK o CLI
- Úselo DeleteEmailIdentity con un AWS SDK o CLI
- Úselo DeleteEmailTemplate con un AWS SDK o CLI
- Úselo GetEmailIdentity con un AWS SDK o CLI
- Úselo ListContactLists con un AWS SDK o CLI
- Úselo ListContacts con un AWS SDK o CLI
- Úselo SendEmail con un AWS SDK o CLI

Úselo **`CreateContact`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `CreateContact`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Flujo de trabajo de

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
    }
```

- Para obtener más información sobre la API, consulta CreateContactla Referencia AWS SDK for .NET de la API.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
    try {
      // Create a new contact with the provided email address in the
```

```
        CreateContactRequest contactRequest = CreateContactRequest.builder()
            .contactListName(CONTACT_LIST_NAME)
            .emailAddress(emailAddress)
            .build();

        sesClient.createContact(contactRequest);
        contacts.add(emailAddress);

        System.out.println("Contact created: " + emailAddress);

        // Send a welcome email to the new contact
        String welcomeHtml = Files.readString(Paths.get("resources/
coupon_newsletter/welcome.html"));
        String welcomeText = Files.readString(Paths.get("resources/
coupon_newsletter/welcome.txt"));

        SendEmailRequest welcomeEmailRequest = SendEmailRequest.builder()
            .fromEmailAddress(this.verifiedEmail)
            .destination(Destination.builder().toAddresses(emailAddress).build())
            .content(EmailContent.builder()
                .simple(
                    Message.builder()
                        .subject(Content.builder().data("Welcome to the Weekly
 Coupons Newsletter").build())
                        .body(Body.builder()
                            .text(Content.builder().data(welcomeText).build())
                            .html(Content.builder().data(welcomeHtml).build())
                            .build())
                        .build())
                .build())
            .build();
        SendEmailResponse welcomeEmailResponse =
 sesClient.sendEmail(welcomeEmailRequest);
        System.out.println("Welcome email sent: " +
 welcomeEmailResponse.messageId());
      } catch (AlreadyExistsException e) {
        // If the contact already exists, skip this step for that contact and
 proceed
        // with the next contact
        System.out.println("Contact already exists, skipping creation...");
      } catch (Exception e) {
        System.err.println("Error occurred while processing email address " +
 emailAddress + ": " + e.getMessage());
        throw e;
```

```
      }
    }
```

- Para obtener más información sobre la API, consulta CreateContactla Referencia AWS SDK for Java 2.x de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta CreateContactla AWS Referencia de API de SDK for Python (Boto3).

Rust

SDK para Rust

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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(())
}
```

- Para obtener más información sobre la API, consulta CreateContactla referencia sobre la API de AWS SDK para Rust.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`CreateContactList`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `CreateContactList`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Flujo de trabajo de

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
    }
```

- Para obtener más información sobre la API, consulta CreateContactListla Referencia AWS SDK for .NET de la API.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
    }
```

- Para obtener más información sobre la API, consulta CreateContactListla Referencia AWS SDK for Java 2.x de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta CreateContactListla AWS Referencia de API de SDK for Python (Boto3).

Rust

SDK para Rust

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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(())
```

```
}
```

- Para obtener más información sobre la API, consulta CreateContactListla referencia sobre la API de AWS SDK para Rust.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`CreateEmailIdentity`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `CreateEmailIdentity`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Flujo de trabajo de

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
        }
    }
```

- Para obtener más información sobre la API, consulta CreateEmailIdentityla Referencia AWS SDK for .NET de la API.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
        }
```

- Para obtener más información sobre la API, consulta CreateEmailIdentityla Referencia AWS SDK for Java 2.x de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta CreateEmailIdentityla AWS Referencia de API de SDK for Python (Boto3).

Rust

SDK para Rust

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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)),
            },
        }
```

- Para obtener más información sobre la API, consulta CreateEmailIdentityla referencia sobre la API de AWS SDK para Rust.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`CreateEmailTemplate`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `CreateEmailTemplate`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Flujo de trabajo de

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
    }
```

- Para obtener más información sobre la API, consulta CreateEmailTemplatela Referencia AWS SDK for .NET de la API.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
    }
```

- Para obtener más información sobre la API, consulta CreateEmailTemplatela Referencia AWS SDK for Java 2.x de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta CreateEmailTemplatela AWS Referencia de API de SDK for Python (Boto3).

Rust

SDK para Rust

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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)),
            },
        }
```

- Para obtener más información sobre la API, consulta CreateEmailTemplatela referencia sobre la API de AWS SDK para Rust.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`DeleteContactList`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DeleteContactList`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Flujo de trabajo de

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
    }
```

- Para obtener más información sobre la API, consulta DeleteContactListla Referencia AWS SDK for .NET de la API.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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();
   }
```

- Para obtener más información sobre la API, consulta DeleteContactListla Referencia AWS SDK for Java 2.x de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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)
```

- Para obtener más información sobre la API, consulta DeleteContactListla AWS Referencia de API de SDK for Python (Boto3).

Rust

SDK para Rust

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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}")),
        }
```

- Para obtener más información sobre la API, consulta DeleteContactListla referencia sobre la API de AWS SDK para Rust.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`DeleteEmailIdentity`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DeleteEmailIdentity`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Flujo de trabajo de

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
    }
```

- Para obtener más información sobre la API, consulta DeleteEmailIdentityla Referencia AWS SDK for .NET de la API.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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.");
    }
```

- Para obtener más información sobre la API, consulta DeleteEmailIdentityla Referencia AWS SDK for Java 2.x de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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)
```

- Para obtener más información sobre la API, consulta DeleteEmailIdentityla AWS Referencia de API de SDK for Python (Boto3).

Rust

SDK para Rust

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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));
                }
            }
```

- Para obtener más información sobre la API, consulta DeleteEmailIdentityla referencia sobre la API de AWS SDK para Rust.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`DeleteEmailTemplate`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `DeleteEmailTemplate`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Flujo de trabajo de

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
    }
```

- Para obtener más información sobre la API, consulta DeleteEmailTemplatela Referencia AWS SDK for .NET de la API.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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();
    }
```

- Para obtener más información sobre la API, consulta DeleteEmailTemplatela Referencia AWS SDK for Java 2.x de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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)
```

- Para obtener más información sobre la API, consulta DeleteEmailTemplatela AWS Referencia de API de SDK for Python (Boto3).

Rust

SDK para Rust

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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}"));
            }
        }
```

- Para obtener más información sobre la API, consulta DeleteEmailTemplatela referencia sobre la API de AWS SDK para Rust.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`GetEmailIdentity`** con un AWS SDK o CLI

En el siguiente ejemplo de código, se muestra cómo usar `GetEmailIdentity`.

Rust

SDK para Rust

> **Note**
>
> Hay más información GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Determina si se ha verificado una dirección de correo electrónico.

```
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(())
}
```

- Para obtener más información sobre la API, consulta GetEmailIdentityla referencia sobre la API de AWS SDK para Rust.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`ListContactLists`** con un AWS SDK o CLI

En el siguiente ejemplo de código, se muestra cómo usar `ListContactLists`.

Rust

SDK para Rust

> **Note**
>
> Hay más información GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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(())
}
```

- Para obtener más información sobre la API, consulta ListContactListsla referencia sobre la API de AWS SDK para Rust.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`ListContacts`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `ListContacts`.

Los ejemplos de acciones son extractos de código de programas más grandes y deben ejecutarse en contexto. Puede ver esta acción en contexto en el siguiente ejemplo de código:

- Flujo de trabajo de

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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>();
    }
```

- Para obtener más información sobre la API, consulta ListContactsla Referencia AWS SDK for .NET de la API.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
      }
```

- Para obtener más información sobre la API, consulta ListContactsla Referencia AWS SDK for Java 2.x de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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
```

- Para obtener más información sobre la API, consulta ListContactsla AWS Referencia de API de SDK for Python (Boto3).

Rust

SDK para Rust

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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(())
}
```

- Para obtener más información sobre la API, consulta ListContactsla referencia sobre la API de AWS SDK para Rust.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Úselo **`SendEmail`** con un AWS SDK o CLI

En los siguientes ejemplos de código, se muestra cómo utilizar `SendEmail`.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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;
    }
```

- Para obtener más información sobre la API, consulta SendEmailla Referencia AWS SDK for .NET de la API.

Java

SDK para Java 2.x

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Envía un mensaje.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.sesv2.model.Body;
import software.amazon.awssdk.services.sesv2.model.Content;
import software.amazon.awssdk.services.sesv2.model.Destination;
import software.amazon.awssdk.services.sesv2.model.EmailContent;
import software.amazon.awssdk.services.sesv2.model.Message;
import software.amazon.awssdk.services.sesv2.model.SendEmailRequest;
import software.amazon.awssdk.services.sesv2.model.SesV2Exception;
import software.amazon.awssdk.services.sesv2.SesV2Client;

/**
 * Before running this AWS SDK for Java (v2) example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
```

```
 */

public class SendEmail {
        public static void main(String[] args) {
                final String usage = """

                                Usage:
                                    <sender> <recipient> <subject>\s

                                Where:
                                    sender - An email address that represents the
 sender.\s
                                    recipient - An email address that represents
 the recipient.\s
                                    subject - The subject line.\s
                                """;

                if (args.length != 3) {
                        System.out.println(usage);
                        System.exit(1);
                }

                String sender = args[0];
                String recipient = args[1];
                String subject = args[2];

                Region region = Region.US_EAST_1;
                SesV2Client sesv2Client = SesV2Client.builder()
                                .region(region)
                                .build();

                // The HTML body of the email.
                String bodyHTML = "<html>" + "<head></head>" + "<body>" +
 "<h1>Hello!</h1>"
                                + "<p> See the list of customers.</p>" + "</
body>" + "</html>";

                send(sesv2Client, sender, recipient, subject, bodyHTML);
        }

        public static void send(SesV2Client client,
                        String sender,
                        String recipient,
                        String subject,
```

```
                        String bodyHTML) {

                Destination destination = Destination.builder()
                                .toAddresses(recipient)
                                .build();

                Content content = Content.builder()
                                .data(bodyHTML)
                                .build();

                Content sub = Content.builder()
                                .data(subject)
                                .build();

                Body body = Body.builder()
                                .html(content)
                                .build();

                Message msg = Message.builder()
                                .subject(sub)
                                .body(body)
                                .build();

                EmailContent emailContent = EmailContent.builder()
                                .simple(msg)
                                .build();

                SendEmailRequest emailRequest = SendEmailRequest.builder()
                                .destination(destination)
                                .content(emailContent)
                                .fromEmailAddress(sender)
                                .build();

                try {
                        System.out.println("Attempting to send an email through
Amazon SES "
                                        + "using the AWS SDK for Java...");
                        client.sendEmail(emailRequest);
                        System.out.println("email was sent");

                } catch (SesV2Exception e) {
                        System.err.println(e.awsErrorDetails().errorMessage());
                        System.exit(1);
                }
```

```
        }
}
```

Envía un mensaje mediante una plantilla.

```
      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());
      }
```

- Para obtener más información sobre la API, consulte SendEmailla Referencia AWS SDK for Java 2.x de la API.

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Envía un mensaje a todos los miembros de la lista de contactos.

```
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}'.")
```

Envía un mensaje a todos los miembros de la lista de contactos mediante una plantilla.

```
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},
                )
```

- Para obtener más información sobre la API, consulta SendEmailla AWS Referencia de API de SDK for Python (Boto3).

Ruby

SDK para Ruby

> **Note**
>
> Hay más información al respecto. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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)
```

- Para obtener más información sobre la API, consulta SendEmailla Referencia AWS SDK for Ruby de la API.

Rust

SDK para Rust

> **Note**
>
> Hay más información al respecto GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Envía un mensaje a todos los miembros de la lista de contactos.

```
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(())
}
```

Envía un mensaje a todos los miembros de la lista de contactos mediante una plantilla.

```
            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)),
            }
```

- Para obtener más información sobre la API, consulte SendEmailla referencia sobre la API de AWS SDK para Rust.

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Escenarios para la API v2 de Amazon SES con AWS SDK

Los siguientes ejemplos de código muestran cómo implementar escenarios comunes en la API v2 de Amazon SES con AWS SDK. Estos escenarios muestran cómo realizar tareas específicas mediante la llamada a varias funciones de la API v2 de Amazon SES. Cada escenario incluye un enlace a GitHub, donde puede encontrar instrucciones sobre cómo configurar y ejecutar el código.

Ejemplos

- Un flujo de trabajo completo para el boletín de Amazon SES API v2 mediante un AWS SDK

Un flujo de trabajo completo para el boletín de Amazon SES API v2 mediante un AWS SDK

Los siguientes ejemplos de código muestran cómo usar el flujo de trabajo de los boletines de Amazon SES API v2.

.NET

AWS SDK for .NET

> **Note**
>
> Hay más información GitHub. Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

Ejecute el flujo de trabajo.

```
using System.Diagnostics;
using System.Text.RegularExpressions;
using Amazon.SimpleEmailV2;
using Amazon.SimpleEmailV2.Model;
```

```
using Microsoft.Extensions.DependencyInjection;
using Microsoft.Extensions.Hosting;
using Microsoft.Extensions.Logging;
using Microsoft.Extensions.Logging.Console;
using Microsoft.Extensions.Logging.Debug;

namespace Sesv2Scenario;

public static class NewsletterWorkflow
{
    /*
      This workflow demonstrates how to use the Amazon Simple Email Service (SES)
 v2 to send a coupon newsletter to a list of subscribers.
      The workflow performs the following tasks:

      1. Prepare the application:
         - Create a verified email identity for sending and replying to emails.
         - Create a contact list to store the subscribers' email addresses.
         - Create an email template for the coupon newsletter.

      2. Gather subscriber email addresses:
         - Prompt the user for a base email address.
         - Create 3 variants of the email address using subaddress extensions
 (e.g., user+ses-weekly-newsletter-1@example.com).
         - Add each variant as a contact to the contact list.
         - Send a welcome email to each new contact.

      3. Send the coupon newsletter:
         - Retrieve the list of contacts from the contact list.
         - Send the coupon newsletter using the email template to each contact.

      4. Monitor and review:
         - Provide instructions for the user to review the sending activity and
 metrics in the AWS console.

      5. Clean up resources:
         - Delete the contact list (which also deletes all contacts within it).
         - Delete the email template.
         - Optionally delete the verified email identity.

    */

    public static SESv2Wrapper _sesv2Wrapper;
    public static string? _baseEmailAddress = null;
```

```
    public static string? _verifiedEmail = null;
    private static string _contactListName = "weekly-coupons-newsletter";
    private static string _templateName = "weekly-coupons";
    private static string _subject = "Weekly Coupons Newsletter";
    private static string _htmlContentFile = "coupon-newsletter.html";
    private static string _textContentFile = "coupon-newsletter.txt";
    private static string _htmlWelcomeFile = "welcome.html";
    private static string _textWelcomeFile = "welcome.txt";
    private static string _couponsDataFile = "sample_coupons.json";

    // Relative location of the shared workflow resources folder.
    private static string _resourcesFilePathLocation = "../../../../../../../
workflows/sesv2_weekly_mailer/resources/";

    public static async Task Main(string[] args)
    {
        // Set up dependency injection for the Amazon service.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureLogging(logging =>
                logging.AddFilter("System", LogLevel.Debug)
                    .AddFilter<DebugLoggerProvider>("Microsoft",
 LogLevel.Information)
                    .AddFilter<ConsoleLoggerProvider>("Microsoft",
 LogLevel.Trace))
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonSimpleEmailServiceV2>()
                    .AddTransient<SESv2Wrapper>()
            )
            .Build();

        ServicesSetup(host);

        try
        {
            Console.WriteLine(new string('-', 80));
            Console.WriteLine(new string('-', 80));
            Console.WriteLine("Welcome to the Amazon SES v2 Coupon Newsletter
 Workflow.");
            Console.WriteLine("This workflow demonstrates how to use the Amazon
 Simple Email Service (SES) v2 " +
                              "\r\nto send a coupon newsletter to a list of
 subscribers.");

            // Prepare the application.
```

```
            var emailIdentity = await PrepareApplication();

            // Gather subscriber email addresses.
            await GatherSubscriberEmailAddresses(emailIdentity);

            // Send the coupon newsletter.
            await SendCouponNewsletter(emailIdentity);

            // Monitor and review.
            MonitorAndReview(true);

            // Clean up resources.
            await Cleanup(emailIdentity, true);

            Console.WriteLine(new string('-', 80));
            Console.WriteLine("Amazon SES v2 Coupon Newsletter Workflow is
complete.");
            Console.WriteLine(new string('-', 80));
            Console.WriteLine(new string('-', 80));
        }
        catch (Exception ex)
        {
            Console.WriteLine($"An error occurred: {ex.Message}");
        }
    }

    /// <summary>
    /// Populate the services for use within the console application.
    /// </summary>
    /// <param name="host">The services host.</param>
    private static void ServicesSetup(IHost host)
    {
        _sesv2Wrapper = host.Services.GetRequiredService<SESv2Wrapper>();
    }

    /// <summary>
    /// Set up the resources for the workflow.
    /// </summary>
    /// <returns>The email address of the verified identity.</returns>
    public static async Task<string?> PrepareApplication()
    {
        var htmlContent = await File.ReadAllTextAsync(_resourcesFilePathLocation
+ _htmlContentFile);
```

```
        var textContent = await File.ReadAllTextAsync(_resourcesFilePathLocation
+ _textContentFile);

        Console.WriteLine(new string('-', 80));
        Console.WriteLine("1. In this step, we will prepare the application:" +
                          "\r\n  - Create a verified email identity for sending
and replying to emails." +
                          "\r\n  - Create a contact list to store the
subscribers' email addresses." +
                          "\r\n  - Create an email template for the coupon
newsletter.\r\n");

        // Prompt the user for a verified email address.
        while (!IsEmail(_verifiedEmail))
        {
            Console.Write("Enter a verified email address or an email to verify:
");
            _verifiedEmail = Console.ReadLine();
        }

        try
        {
            // Create an email identity and start the verification process.
            await _sesv2Wrapper.CreateEmailIdentityAsync(_verifiedEmail);
            Console.WriteLine($"Identity {_verifiedEmail} created.");
        }
        catch (AlreadyExistsException)
        {
            Console.WriteLine($"Identity {_verifiedEmail} already exists.");
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Error creating email identity: {ex.Message}");
        }

        // Create a contact list.
        try
        {
            await _sesv2Wrapper.CreateContactListAsync(_contactListName);
            Console.WriteLine($"Contact list {_contactListName} created.");
        }
        catch (AlreadyExistsException)
        {
```

```
            Console.WriteLine($"Contact list {_contactListName} already
exists.");
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Error creating contact list: {ex.Message}");
        }

        // Create an email template.
        try
        {
            await _sesv2Wrapper.CreateEmailTemplateAsync(_templateName, _subject,
htmlContent, textContent);
            Console.WriteLine($"Email template {_templateName} created.");
        }
        catch (AlreadyExistsException)
        {
            Console.WriteLine($"Email template {_templateName} already exists.");
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Error creating email template: {ex.Message}");
        }

        return _verifiedEmail;
    }

    /// <summary>
    /// Generate subscriber addresses and send welcome emails.
    /// </summary>
    /// <param name="fromEmailAddress">The verified email address from
PrepareApplication.</param>
    /// <returns>True if successful.</returns>
    public static async Task<bool> GatherSubscriberEmailAddresses(string
fromEmailAddress)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine("2. In Step 2, we will gather subscriber email
addresses:" +
                          "\r\n  - Prompt the user for a base email address." +
                          "\r\n  - Create 3 variants of the email address using
subaddress extensions (e.g., user+ses-weekly-newsletter-1@example.com)." +
                          "\r\n  - Add each variant as a contact to the contact
list." +
```

```
                        "\r\n  - Send a welcome email to each new contact.\r
\n");

        // Prompt the user for a base email address.
        while (!IsEmail(_baseEmailAddress))
        {
            Console.Write("Enter a base email address (e.g., user@example.com):
 ");
            _baseEmailAddress = Console.ReadLine();
        }

        // Create 3 variants of the email address using +ses-weekly-newsletter-1,
 +ses-weekly-newsletter-2, etc.
        var baseEmailAddressParts = _baseEmailAddress!.Split("@");
        for (int i = 1; i <= 3; i++)
        {
            string emailAddress = $"{baseEmailAddressParts[0]}+ses-weekly-
newsletter-{i}@{baseEmailAddressParts[1]}";

            try
            {
                // Create a contact with the email address in the contact list.
                await _sesv2Wrapper.CreateContactAsync(emailAddress,
 _contactListName);
                Console.WriteLine($"Contact {emailAddress} added to the
 {_contactListName} contact list.");
            }
            catch (AlreadyExistsException)
            {
                Console.WriteLine($"Contact {emailAddress} already exists in the
 {_contactListName} contact list.");
            }
            catch (Exception ex)
            {
                Console.WriteLine($"Error creating contact {emailAddress}:
 {ex.Message}");
                return false;
            }

            // Send a welcome email to the new contact.
            try
            {
                string subject = "Welcome to the Weekly Coupons Newsletter";
```

```
                string htmlContent = await
File.ReadAllTextAsync(_resourcesFilePathLocation + _htmlWelcomeFile);
                string textContent = await
File.ReadAllTextAsync(_resourcesFilePathLocation + _textWelcomeFile);

                await _sesv2Wrapper.SendEmailAsync(fromEmailAddress, new
List<string> { emailAddress }, subject, htmlContent, textContent);
                Console.WriteLine($"Welcome email sent to {emailAddress}.");
            }
            catch (Exception ex)
            {
                Console.WriteLine($"Error sending welcome email to
{emailAddress}: {ex.Message}");
                return false;
            }

            // Wait 2 seconds before sending the next email (if the account is in
the SES Sandbox).
            await Task.Delay(2000);
        }

        return true;
    }

    /// <summary>
    ///  Send the coupon newsletter to the subscribers in the contact list.
    /// </summary>
    /// <param name="fromEmailAddress">The verified email address from
PrepareApplication.</param>
    /// <returns>True if successful.</returns>
    public static async Task<bool> SendCouponNewsletter(string fromEmailAddress)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine("3. In this step, we will send the coupon newsletter:"
+
                          "\r\n  - Retrieve the list of contacts from the contact
list." +
                          "\r\n  - Send the coupon newsletter using the email
template to each contact.\r\n");


        // Retrieve the list of contacts from the contact list.
        var contacts = await _sesv2Wrapper.ListContactsAsync(_contactListName);
        if (!contacts.Any())
```

```
        {
            Console.WriteLine($"No contacts found in the {_contactListName}
contact list.");
            return false;
        }

        // Load the coupon data from the sample_coupons.json file.
        string couponsData = await
File.ReadAllTextAsync(_resourcesFilePathLocation + _couponsDataFile);

        // Send the coupon newsletter to each contact using the email template.
        try
        {
            foreach (var contact in contacts)
            {
                // To use the Contact List for list management, send to only one
address at a time.
                await _sesv2Wrapper.SendEmailAsync(fromEmailAddress,
                    new List<string> { contact.EmailAddress },
                    null, null, null, _templateName, couponsData,
_contactListName);
            }

            Console.WriteLine($"Coupon newsletter sent to contact list
{_contactListName}.");
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Error sending coupon newsletter to contact list
{_contactListName}: {ex.Message}");
            return false;
        }

        return true;
    }

    /// <summary>
    /// Provide instructions for monitoring sending activity and metrics.
    /// </summary>
    /// <param name="interactive">True to run in interactive mode.</param>
    /// <returns>True if successful.</returns>
    public static bool MonitorAndReview(bool interactive)
    {
        Console.WriteLine(new string('-', 80));
```

```
        Console.WriteLine("4. In step 4, we will monitor and review:" +
                          "\r\n  - Provide instructions for the user to review
the sending activity and metrics in the AWS console.\r\n");

        Console.WriteLine("Review your sending activity using the SES Homepage in
the AWS console.");
        Console.WriteLine("Press Enter to open the SES Homepage in your default
browser...");
        if (interactive)
        {
            Console.ReadLine();
            try
            {
                // Open the SES Homepage in the default browser.
                Process.Start(new ProcessStartInfo
                {
                    FileName = "https://console.aws.amazon.com/ses/home",
                    UseShellExecute = true
                });
            }
            catch (Exception ex)
            {
                Console.WriteLine($"Error opening the SES Homepage:
{ex.Message}");
                return false;
            }
        }

        Console.WriteLine("Review the sending activity and email metrics, then
press Enter to continue...");
        if (interactive)
            Console.ReadLine();
        return true;
    }

    /// <summary>
    /// Clean up the resources used in the workflow.
    /// </summary>
    /// <param name="verifiedEmailAddress">The verified email address from
PrepareApplication.</param>
    /// <param name="interactive">True if interactive.</param>
    /// <returns>Async task.</returns>
    public static async Task<bool> Cleanup(string verifiedEmailAddress, bool
interactive)
```

```
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine("5. Finally, we clean up resources:" +
                          "\r\n  - Delete the contact list (which also deletes
 all contacts within it)." +
                          "\r\n  - Delete the email template." +
                          "\r\n  - Optionally delete the verified email identity.
\r\n");

        Console.WriteLine("Cleaning up resources...");

        // Delete the contact list (this also deletes all contacts in the list).
        try
        {
            await _sesv2Wrapper.DeleteContactListAsync(_contactListName);
            Console.WriteLine($"Contact list {_contactListName} deleted.");
        }
        catch (NotFoundException)
        {
            Console.WriteLine($"Contact list {_contactListName} not found.");
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Error deleting contact list {_contactListName}:
 {ex.Message}");
            return false;
        }

        // Delete the email template.
        try
        {
            await _sesv2Wrapper.DeleteEmailTemplateAsync(_templateName);
            Console.WriteLine($"Email template {_templateName} deleted.");
        }
        catch (NotFoundException)
        {
            Console.WriteLine($"Email template {_templateName} not found.");
        }
        catch (Exception ex)
        {
            Console.WriteLine($"Error deleting email template {_templateName}:
 {ex.Message}");
            return false;
        }
```

```
        // Ask the user if they want to delete the email identity.
        var deleteIdentity = !interactive ||
            GetYesNoResponse(
                $"Do you want to delete the email identity
 {verifiedEmailAddress}? (y/n) ");
        if (deleteIdentity)
        {
            try
            {
                await
 _sesv2Wrapper.DeleteEmailIdentityAsync(verifiedEmailAddress);
                Console.WriteLine($"Email identity {verifiedEmailAddress}
 deleted.");
            }
            catch (NotFoundException)
            {
                Console.WriteLine(
                    $"Email identity {verifiedEmailAddress} not found.");
            }
            catch (Exception ex)
            {
                Console.WriteLine(
                    $"Error deleting email identity {verifiedEmailAddress}:
 {ex.Message}");
                return false;
            }
        }
        else
        {
            Console.WriteLine(
                $"Skipping deletion of email identity {verifiedEmailAddress}.");
        }

        return true;
    }

    /// <summary>
    /// Helper method to get a yes or no response from the user.
    /// </summary>
    /// <param name="question">The question string to print on the console.</
param>
    /// <returns>True if the user responds with a yes.</returns>
    private static bool GetYesNoResponse(string question)
```

```
    {
        Console.WriteLine(question);
        var ynResponse = Console.ReadLine();
        var response = ynResponse != null && ynResponse.Equals("y",
 StringComparison.InvariantCultureIgnoreCase);
        return response;
    }

    /// <summary>
    /// Simple check to verify a string is an email address.
    /// </summary>
    /// <param name="email">The string to verify.</param>
    /// <returns>True if a valid email.</returns>
    private static bool IsEmail(string? email)
    {
        if (string.IsNullOrEmpty(email))
            return false;
        return Regex.IsMatch(email, @"^[^@\s]+@[^@\s]+\.[^@\s]+$",
 RegexOptions.IgnoreCase);
    }
}
```

Envoltorio para operaciones de servicio.

```
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;
    }
}
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de la API de AWS SDK for .NET .
  - CreateContact
  - CreateContactList
  - CreateEmailIdentity
  - CreateEmailTemplate
  - DeleteContactList
  - DeleteEmailIdentity
  - DeleteEmailTemplate
  - ListContacts
  - SendEmail.simple
  - SendEmail.plantilla

Java

SDK para Java 2.x

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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();
        }
```

- Para obtener información sobre la API, consulte los siguientes temas en la referencia de la API de AWS SDK for Java 2.x .
  - CreateContact
  - CreateContactList
  - CreateEmailIdentity
  - CreateEmailTemplate
  - DeleteContactList
  - DeleteEmailIdentity
  - DeleteEmailTemplate
  - ListContacts
  - SendEmail.simple
  - SendEmail.plantilla

Python

SDK para Python (Boto3)

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de AWS.

```
def main():
    """
    The main function that orchestrates the execution of the workflow.
    """
    print(INTRO)
    ses_client = boto3.client("sesv2")
    workflow = SESv2Workflow(ses_client)
    try:
        workflow.prepare_application()
        workflow.gather_subscriber_email_addresses()
```

```
        workflow.send_coupon_newsletter()
        workflow.monitor_and_review()
    except ClientError as e:
        print_error(e)
    workflow.clean_up()



class SESv2Workflow:
    """
    A class to manage the SES v2 Coupon Newsletter Workflow.
    """

    def __init__(self, ses_client, sleep=True):
        self.ses_client = ses_client
        self.sleep = sleep


        try:

 self.ses_client.create_contact_list(ContactListName=CONTACT_LIST_NAME)
            print(f"Contact list '{CONTACT_LIST_NAME}' created successfully.")
        except ClientError as e:
            # If the contact list already exists, skip and proceed
            if e.response["Error"]["Code"] == "AlreadyExistsException":
                print(f"Contact list '{CONTACT_LIST_NAME}' already exists.")
            else:
                raise e

            try:
                # Create a new contact
                self.ses_client.create_contact(
                    ContactListName=CONTACT_LIST_NAME, EmailAddress=email
                )
                print(f"Contact with email '{email}' created successfully.")

                # Send the welcome email
                self.ses_client.send_email(
                    FromEmailAddress=self.verified_email,
                    Destination={"ToAddresses": [email]},
                    Content={
                        "Simple": {
                            "Subject": {
```

```
                                "Data": "Welcome to the Weekly Coupons
Newsletter"
                            },
                            "Body": {
                                "Text": {"Data": welcome_text},
                                "Html": {"Data": welcome_html},
                            },
                        }
                    },
                )
                print(f"Welcome email sent to '{email}'.")
                if self.sleep:
                    # 1 email per second in sandbox mode, remove in production.
                    sleep(1.1)
            except ClientError as e:
                # If the contact already exists, skip and proceed
                if e.response["Error"]["Code"] == "AlreadyExistsException":
                    print(f"Contact with email '{email}' already exists.
Skipping...")
                else:
                    raise e

        try:
            contacts_response = self.ses_client.list_contacts(
                ContactListName=CONTACT_LIST_NAME
            )
        except ClientError as e:
            if e.response["Error"]["Code"] == "NotFoundException":
                print(f"Contact list '{CONTACT_LIST_NAME}' does not exist.")
                return
            else:
                raise e

                self.ses_client.send_email(
                    FromEmailAddress=self.verified_email,
                    Destination={"ToAddresses": [email]},
                    Content={
                        "Simple": {
                            "Subject": {
                                "Data": "Welcome to the Weekly Coupons
Newsletter"
                            },
                            "Body": {
                                "Text": {"Data": welcome_text},
```

```
                                "Html": {"Data": welcome_html},
                            },
                        }
                    },
                )
                print(f"Welcome email sent to '{email}'.")

                self.ses_client.send_email(
                    FromEmailAddress=self.verified_email,
                    Destination={"ToAddresses": [email_address]},
                    Content={
                        "Template": {
                            "TemplateName": TEMPLATE_NAME,
                            "TemplateData": coupon_items,
                        }
                    },
                    ListManagementOptions={"ContactListName": CONTACT_LIST_NAME},
                )

        try:

self.ses_client.create_email_identity(EmailIdentity=self.verified_email)
            print(f"Email identity '{self.verified_email}' created
successfully.")
        except ClientError as e:
            # If the email identity already exists, skip and proceed
            if e.response["Error"]["Code"] == "AlreadyExistsException":
                print(f"Email identity '{self.verified_email}' already exists.")
            else:
                raise e

        try:
            template_content = {
                "Subject": "Weekly Coupons Newsletter",
                "Html": load_file_content("coupon-newsletter.html"),
                "Text": load_file_content("coupon-newsletter.txt"),
            }
            self.ses_client.create_email_template(
                TemplateName=TEMPLATE_NAME, TemplateContent=template_content
            )
            print(f"Email template '{TEMPLATE_NAME}' created successfully.")
        except ClientError as e:
            # If the template already exists, skip and proceed
            if e.response["Error"]["Code"] == "AlreadyExistsException":
```

```
                print(f"Email template '{TEMPLATE_NAME}' already exists.")
            else:
                raise e

        try:

self.ses_client.delete_contact_list(ContactListName=CONTACT_LIST_NAME)
            print(f"Contact list '{CONTACT_LIST_NAME}' deleted successfully.")
        except ClientError as e:
            # If the contact list doesn't exist, skip and proceed
            if e.response["Error"]["Code"] == "NotFoundException":
                print(f"Contact list '{CONTACT_LIST_NAME}' does not exist.")
            else:
                print(e)

            try:

self.ses_client.delete_email_identity(EmailIdentity=self.verified_email)
                print(f"Email identity '{self.verified_email}' deleted
successfully.")
            except ClientError as e:
                # If the email identity doesn't exist, skip and proceed
                if e.response["Error"]["Code"] == "NotFoundException":
                    print(f"Email identity '{self.verified_email}' does not
exist.")
                else:
                    print(e)

        try:
            self.ses_client.delete_email_template(TemplateName=TEMPLATE_NAME)
            print(f"Email template '{TEMPLATE_NAME}' deleted successfully.")
        except ClientError as e:
            # If the email template doesn't exist, skip and proceed
            if e.response["Error"]["Code"] == "NotFoundException":
                print(f"Email template '{TEMPLATE_NAME}' does not exist.")
            else:
                print(e)
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de la API de AWS SDK para Python (Boto3).
  - CreateContact

- CreateContactList
- CreateEmailIdentity
- CreateEmailTemplate
- DeleteContactList
- DeleteEmailIdentity
- DeleteEmailTemplate
- ListContacts
- SendEmail.simple
- SendEmail.plantilla

Rust

SDK para Rust

> **Note**
>
> Hay más información. GitHub Busque el ejemplo completo y aprenda a configurar y ejecutar en el Repositorio de ejemplos de código de 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}"));
            }
        }
```

- Para obtener información sobre la API, consulte los siguientes temas en la Referencia de la API de AWS SDK para Rust.
  - CreateContact
  - CreateContactList
  - CreateEmailIdentity
  - CreateEmailTemplate
  - DeleteContactList
  - DeleteEmailIdentity
  - DeleteEmailTemplate
  - ListContacts
  - SendEmail.simple
  - SendEmail.plantilla

Para obtener una lista completa de guías para desarrolladores del AWS SDK y ejemplos de código, consulteUso de Amazon SES con un AWS SDK. En este tema también se incluye información sobre cómo comenzar a utilizar el SDK y detalles sobre sus versiones anteriores.

Seguridad en Amazon Simple Email Service

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de conformidad que se aplican a Amazon Simple Email Service, consulte AWS Servicios dentro del alcance por programa de conformidad AWS .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables

Esta documentación lo ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Amazon Simple Email Service. Muestra cómo configurar Amazon Simple Email Service para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de Amazon Simple Email Service.

> **Note**
>
> Si necesita denunciar un uso indebido de AWS los recursos, incluido el correo no deseado o la distribución de software malicioso, no utilice el enlace de comentarios que aparece en ninguna de las páginas de esta guía para desarrolladores, ya que el formulario lo recibe el equipo de AWS documentación, no AWS Trust & Safety. En su lugar, en la página ¿Cómo denuncio un uso indebido de AWS los recursos? página, sigue las instrucciones para ponerte en contacto con el equipo de AWS Confianza y Seguridad para denunciar cualquier tipo de AWS abuso de Amazon.

Contenido

- Protección de datos en Amazon Simple Email Service
- Identity and Access Management en Amazon SES
- Registro y monitoreo en Amazon SES
- Validación de conformidad para Amazon Simple Email Service
- Resiliencia de Amazon Simple Email Service
- Seguridad de la infraestructura en Amazon Simple Email Service
- Configuración de puntos de enlace de la VPC con Amazon SES

Protección de datos en Amazon Simple Email Service

El modelo de se aplica a protección de datos en Amazon Simple Email Service. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información

sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Amazon Simple Email Service u otro servicio Servicios de AWS mediante la consola, la API o AWS los SDK. AWS CLI Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Contenido

- El cifrado de datos en reposo para Amazon SES
- Cifrado en tránsito
- Eliminación de datos personales de Amazon SES

El cifrado de datos en reposo para Amazon SES

De forma predeterminada, Amazon SES cifra todos los datos en reposo. El cifrado predeterminado ayuda a reducir la sobrecarga operativa y la complejidad que implica la protección de los datos. El cifrado también le permite crear archivos de Mail Manager que cumplen con los estrictos requisitos normativos y de conformidad con el cifrado.

SES ofrece las siguientes opciones de cifrado:

- AWS claves propias: SES las usa de forma predeterminada. No puede ver, administrar ni usar las claves AWS propias, ni auditar su uso. Sin embargo, no tiene que realizar ninguna acción ni cambiar ningún programa para proteger las claves que cifran sus datos. Para obtener más información, consulte las claves propiedad de AWS en la Guía para desarrolladores de AWS Key Management Service .
- Claves administradas por el cliente: SES admite el uso de claves simétricas administradas por el cliente que usted crea, posee y administra. Como usted tiene el control total del cifrado, puede realizar tareas como:
  - Establecer y mantener políticas de claves
  - Establecer y mantener concesiones y políticas de IAM

- Habilitar y deshabilitar políticas de claves
- Rotar el material criptográfico
- Agregar etiquetas.
- Crear alias de clave
- Programar la eliminación de claves

Para usar su propia clave, elija una clave administrada por el cliente al crear sus recursos de SES.

Para más información, consulte las claves administradas por el cliente en la Guía para desarrolladores de AWS Key Management Service .

> **Note**
>
> SES habilita automáticamente el cifrado en reposo utilizando claves AWS propias sin coste alguno.
> Sin embargo, se aplican AWS KMS cargos por el uso de una clave administrada por el cliente. Para obtener más información acerca de los precios, consulte Precios de AWS Key Management Service.

Crear una clave administrada por el cliente

Puede crear una clave simétrica gestionada por el cliente mediante las AWS Management Console API o las AWS KMS API.

Para crear una clave simétrica administrada por el cliente

Siga los pasos para crear claves KMS de cifrado simétrico de la Guía para AWS Key Management Service desarrolladores.

> **Note**
>
> Para archivar, la clave debe cumplir los siguientes requisitos:
>
> - La clave debe ser simétrica.
> - El origen del material clave debe ser. `AWS_KMS`
> - El uso de la clave debe ser`ENCRYPT_DECRYPT`.

Política de claves

Las políticas de clave controlan el acceso a la clave administrada por el cliente. Cada clave administrada por el cliente debe tener exactamente una política de clave, que contiene instrucciones que determinan quién puede usar la clave y cómo puede utilizarla. Cuando crea la clave administrada por el cliente, puede especificar una política de clave. Para obtener más información, consulte Administración del acceso a las claves en la Guía para desarrolladores de AWS Key Management Service .

Para utilizar la clave gestionada por el cliente con el archivado de Mail Manager, la política de claves debe permitir las siguientes operaciones de API:

- kms: DescribeKey — Proporciona los detalles de la clave administrada por el cliente que permiten a SES validarla.
- kms: GenerateDataKey — Permite a SES generar una clave de datos para cifrar los datos en reposo.
- kms:Decrypt: permite a SES descifrar los datos almacenados antes de devolverlos a los clientes de la API.

El siguiente ejemplo muestra una política de claves típica:

```
{
            "Sid": "Allow SES to encrypt/decrypt",
            "Effect": "Allow",
            "Principal": {
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
```

Para obtener más información, consulte especificar los permisos en una política en la Guía para AWS Key Management Service desarrolladores.

Para obtener más información sobre la solución de problemas, consulte la sección de solución de problemas de acceso a las claves en la Guía para AWS Key Management Service desarrolladores.

Especificar una clave administrada por el cliente para archivar Mail Manager

Puede especificar una clave gestionada por el cliente como alternativa al uso de claves AWS propias. Al crear un archivo, puede especificar la clave de datos introduciendo una clave KMS ARN, que Mail Manager archiving utiliza para cifrar todos los datos de los clientes del archivo.

- ARN de clave KMS: identificador de clave para una clave administrada por el AWS KMS cliente. Introduzca el ID de la clave, el ARN de la clave, el nombre de alias o el ARN del alias.

Contexto de cifrado de Amazon SES

Un contexto de cifrado es un conjunto opcional de pares clave-valor que pueden contener información contextual adicional sobre los datos.

AWS KMS utiliza el contexto de cifrado como datos autenticados adicionales para respaldar el cifrado autenticado. Al incluir un contexto de cifrado en una solicitud de cifrado de datos, AWS KMS vincula el contexto de cifrado a los datos cifrados. Para descifrar los datos, debe incluir el mismo contexto de cifrado en la solicitud.

> **Note**
>
> Amazon SES no admite contextos de cifrado para la creación de archivos. En su lugar, utiliza una política de IAM o KMS. Para ver políticas de ejemploPolíticas de creación de archivos, consulte más adelante en esta sección.

Contexto de cifrado de Amazon SES

SES utiliza el mismo contexto de cifrado en todas las operaciones AWS KMS criptográficas, donde la clave es `aws:ses:arn` y el valor es el Amazon Resource Name (ARN) del recurso.

Example

```
"encryptionContext": {
    "aws:ses:arn": "arn:aws:ses:us-west-2:111122223333:ExampleResourceName/
ExampleResourceID"
}
```

Uso del contexto de cifrado para la supervisión

Si utiliza una clave simétrica gestionada por el cliente para cifrar su recurso de SES, también puede utilizar el contexto de cifrado en los registros y registros de auditoría para identificar cómo se utiliza la clave gestionada por el cliente. El contexto de cifrado también aparece en los registros generados por AWS CloudTrail Amazon CloudWatch Logs.

Utilizar el contexto de cifrado para controlar el acceso a la clave administrada por el cliente

Puede utilizar el contexto de cifrado en las políticas de claves y las políticas de IAM como `conditions` para controlar el acceso a la clave simétrica administrada por el cliente. Puede usar también una restricción de contexto de cifrado en una concesión.

SES utiliza una restricción de contexto de cifrado en las concesiones para controlar el acceso a la clave gestionada por el cliente en su cuenta o región. La restricción de concesión requiere que las operaciones que permite la concesión utilicen el contexto de cifrado especificado.

Example

Los siguientes son ejemplos de declaraciones de política clave para conceder acceso a una clave administrada por el cliente para un contexto de cifrado específico. La condición de esta declaración de política exige que las concesiones tengan una restricción de contexto de cifrado que especifique el contexto de cifrado.

```
{
    "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"
          }
     }
}
```

Políticas de creación de archivos

Los siguientes ejemplos de políticas muestran cómo habilitar la creación de archivos. Las políticas funcionan en todos los activos.

Política de 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 política

```
{
            "Sid": "Allow SES to encrypt/decrypt",
            "Effect": "Allow",
            "Principal": {
```

```
                "Service": "ses.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
```

Supervisión de las claves de cifrado para Amazon SES

Cuando utiliza una clave gestionada por el AWS KMS cliente con sus recursos de Amazon SES, puede utilizar AWS CloudTrailo Amazon CloudWatch Logs para realizar un seguimiento de las solicitudes que SES envía AWS KMS.

Los siguientes ejemplos son AWS CloudTrail eventos para y `DescribeKey` para `GenerateDataKey` monitorear las operaciones de KMS solicitadas por SES para acceder a los datos cifrados por su clave administrada por el cliente: `Decrypt`

GenerateDataKey

Cuando habilita una clave administrada por el AWS KMS cliente para su recurso, SES crea una clave de tabla única. Envía una `GenerateDataKey` solicitud a la AWS KMS que se especifica la clave gestionada por el AWS KMS cliente para el recurso.

Si habilitas una clave gestionada por el AWS KMS cliente para tu recurso de archivo de Mail Manager, `GenerateDataKey` se utilizará para cifrar los datos de archivo en reposo.

El siguiente evento de ejemplo registra la operación `GenerateDataKey`:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "ses.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
```

```
    "requestParameters": {
        "encryptionContext": {
            "aws:ses:arn": "arn:aws:ses:us-west-2:111122223333:ExampleResourceName/
ExampleResourceID"
        },
        "keySpec": "AES_256",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333",
    "sharedEventID": "57f5dbee-16da-413e-979f-2c4c6663475e"
}
```


Decrypt

Al acceder a un recurso cifrado, SES solicita a la `Decrypt` operación que utilice la clave de datos cifrados almacenada para acceder a los datos cifrados.

El siguiente evento de ejemplo registra la operación `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 usa la `DescribeKey` operación para verificar si la clave administrada por el AWS KMS cliente asociada a su recurso existe en la cuenta y la región.

El siguiente evento de ejemplo registra la operación `DescribeKey`:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
```

```
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-04-22T17:02:00Z"
            }
        },
        "invokedBy": "ses.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "keyId": "00dd0db0-0000-0000-ac00-b0c000SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
```

```
}
```

Más información

Los siguientes recursos proporcionan más información sobre cifrado de datos en reposo.

- Para obtener más información acerca de conceptos básicos de AWS Key Management Service, consulte la Guía para desarrolladores de AWS Key Management Service .
- Para obtener más información sobre las prácticas recomendadas de seguridad de AWS Key Management Service, consulte la Guía para desarrolladores de AWS Key Management Service .

Cifrado en tránsito

De forma predeterminada, Amazon SES utiliza TLS de forma oportuna. Esto significa que Amazon SES siempre intenta realizar una conexión segura al servidor de recepción de correo electrónico. Si no puede establecer una conexión segura, envía el mensaje sin cifrar. Puede cambiar este comportamiento para que Amazon SES envíe el mensaje al servidor de correo electrónico receptor solo si puede establecer una conexión segura. Para obtener más información, consulte Amazon SES y los protocolos de seguridad.

Eliminación de datos personales de Amazon SES

En función de cómo lo utilice, Amazon SES puede almacenar determinados datos que podrían considerarse personales. Por ejemplo, para enviar correo electrónico a través de Amazon SES, debe proporcionar al menos una identidad verificada (una dirección o dominio de correo electrónico). Puede utilizar la consola o la API de Amazon SES para eliminar definitivamente estos datos personales.

Este capítulo proporciona procedimientos para eliminar diversos tipos de datos que podrían considerarse personales.

Contenido

- Eliminar direcciones de correo electrónico de la lista de supresión de nivel de cuenta
- Eliminación de datos acerca del correo electrónico enviado con Amazon SES
- Eliminación de datos sobre identidades
- Eliminación de datos de autenticación de remitente

- Eliminación de datos relacionados con las reglas de recepción
- Eliminación de datos relacionados con los filtros de direcciones IP
- Eliminación de datos en plantillas de correo electrónico
- Eliminación de datos en plantillas de correo electrónico de verificación personalizadas
- Elimine todos los datos personales cerrando su AWS cuenta

Eliminar direcciones de correo electrónico de la lista de supresión de nivel de cuenta

Amazon SES incluye una lista de supresión de nivel de cuenta opcional. Cuando se habilita esta característica, las direcciones de correo electrónico se añaden automáticamente a una lista de supresión si los mensajes enviados a ellas rebotan o reciben una reclamación. Las direcciones de correo electrónico permanecen en esta lista hasta que se eliminan. Para obtener más información acerca de la lista de supresión de nivel de cuenta, consulte Uso de la lista de supresión de nivel de cuenta de Amazon SES.

Puede eliminar direcciones de correo electrónico de la lista de supresión de nivel de cuenta mediante la operación `DeleteSuppressedDestination` de la API v2 de Amazon SES. Esta sección incluye un procedimiento para eliminar direcciones de correo electrónico mediante la AWS CLI. Para obtener más información sobre cómo instalar y configurar la AWS CLI, consulte la Guía del usuario de la AWS Command Line Interface.

Para quitar una dirección de la lista de supresión de nivel de cuenta mediante la AWS CLI

- En la línea de comandos, escriba el comando siguiente.

  ```
  aws sesv2 delete-suppressed-destination --email-address recipient@example.com
  ```

  En el comando anterior, sustituya *recipient@example.com* por la dirección de correo electrónico que desea eliminar de la lista de supresión de nivel de cuenta.

Eliminación de datos acerca del correo electrónico enviado con Amazon SES

Cuando utilizas Amazon SES para enviar un correo electrónico, puedes enviar información sobre ese correo electrónico a otros AWS servicios. Por ejemplo, puedes enviar información sobre eventos de correo electrónico (como entregas, aperturas y clics) a Firehose. Estos datos de evento normalmente contienen su dirección de correo electrónico y la dirección IP del correo electrónico desde el que se

envió. También contienen las direcciones de correo electrónico de todos los destinatarios a los que se envió el correo electrónico.

Puede usar Firehose para transmitir datos de eventos de correo electrónico a varios destinos, incluidos Amazon Simple Storage Service, Amazon Service y OpenSearch Amazon Redshift. Para eliminar estos datos, primero debes detener la transmisión de datos a Firehose y, a continuación, eliminar los datos que ya se han transmitido. Para dejar de transmitir los datos del evento de Amazon SES a Firehose, debes eliminar el destino del evento de Firehose.

Para eliminar el destino de un evento de Firehose mediante la consola Amazon SES

1. Abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En Email Sending (Envío de correo electrónico), elija Configuration Sets (Conjuntos de configuración).
3. En la lista de conjuntos de configuración, elija el conjunto de configuraciones que contiene el destino del evento Firehose.
4. Junto al destino del evento Firehose que quieres eliminar, selecciona el botón eliminar ( ).
5. Si es necesario, elimina los datos que Firehose escribió a otros servicios. Para obtener más información, consulte the section called “Quitar datos de eventos de almacenados”.

También puede utilizar la API de Amazon SES para eliminar destinos de eventos. El siguiente procedimiento utiliza AWS Command Line Interface (AWS CLI) para interactuar con la API de Amazon SES. También puede interactuar con la API mediante un AWS SDK o realizando solicitudes HTTP directamente.

Para eliminar el destino de un evento Firehose mediante el AWS CLI

1. En la línea de comando, escriba el comando siguiente:

```
aws sesv2 delete-configuration-set-event-destination --configuration-set-
name configSet \
--event-destination-name eventDestination
```

   En este comando, sustituya *ConfigSet* por el nombre del conjunto de configuraciones que contiene el destino del evento Firehose. Sustituya *EventDestination* por el nombre del destino del evento Firehose.

2. Si es necesario, elimina los datos que Firehose escribió a otros servicios. Para obtener más información, consulte the section called “Quitar datos de eventos de almacenados”.

Quitar datos de eventos de almacenados

Para obtener más información sobre cómo eliminar información de otros AWS servicios, consulte los siguientes documentos:

- Eliminación de un objeto y un bucket en la Guía del usuario de Amazon Simple Storage Service
- Eliminar un dominio OpenSearch de servicio en la Guía para desarrolladores OpenSearch de Amazon Service
- Eliminación de un clúster en la Guía de administración de clústeres de Amazon Redshift

También puedes usar Firehose para transmitir datos de correo electrónico a Splunk, un servicio de terceros que no es compatible AWS ni administrado por. AWS Management Console Para obtener más información acerca de la eliminación de datos de Splunk, consulte al administrador del sistema o la documentación en el sitio web de Splunk.

Eliminación de datos sobre identidades

Las identidades incluyen las direcciones de correo electrónico y los dominios que utiliza para enviar correo electrónico mediante Amazon SES. En algunas jurisdicciones, las direcciones de correo electrónico o los dominios podrían considerarse datos personales.

Para eliminar una identidad con la consola de Amazon SES

1. Abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En Identity Management (Administración de identidad), lleve a cabo una de las siguientes operaciones:
   - Elija Domains (Dominios) si desea eliminar un dominio.
   - Elija Email Addresses (Direcciones de correo electrónico) si desea eliminar una dirección de correo electrónico.
3. Elija la identidad que desee eliminar y, a continuación, elija Remove (Quitar).
4. En el cuadro de diálogo de confirmación, elija Yes, Delete Identity (Sí, eliminar identidad).

También puede utilizar la API de Amazon SES para eliminar identidades. El siguiente procedimiento utiliza la AWS Command Line Interface (AWS CLI) para interactuar con la API de Amazon SES. También puedes interactuar con la API mediante un AWS SDK o realizando solicitudes HTTP directamente.

Para eliminar una identidad mediante el AWS CLI

- En la línea de comando, escriba el comando siguiente:

  ```
  aws ses delete-identity --identity sender@example.com
  ```

  En este comando, reemplace *remitente@ejemplo.com* por la identidad que desea eliminar.

Eliminación de datos de autenticación de remitente

La autenticación del remitente hace referencia al proceso de configurar Amazon SES para que otro usuario pueda enviar correo electrónico en su nombre. Para habilitar la autorización del remitente, debe crear una política, tal y como se describe en Uso de la autorización de envío con Amazon SES. Estas políticas contienen identidades (que le pertenecen), además de AWS identificadores (que están asociados a la persona o grupo que envía el correo electrónico en su nombre). Puede quitar estos datos personales, modificando o eliminando las políticas de autenticación de remitente. Los procedimientos que se describen a continuación muestran cómo eliminar estas políticas.

Para eliminar una política de autenticación de remitente a través de consola de Amazon SES

1. Abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En Identity Management (Administración de identidad), lleve a cabo una de las siguientes operaciones:
   - Elija Domains (Dominios) si la política de autenticación de remitente que desea eliminar está asociada a un dominio.
   - Elija Email Addresses (Direcciones de correo electrónico) si la política de autenticación de remitente que desea eliminar está asociada a una dirección de correo electrónico.
3. En Identity Policies (Políticas de identidad), elija la política que desea eliminar y, a continuación, elija Remove Policy (Quitar política).

Puede utilizar la API de Amazon SES para eliminar las políticas de autenticación de remitente. El siguiente procedimiento utiliza AWS Command Line Interface (AWS CLI) para interactuar con la API de Amazon SES. También puede interactuar con la API mediante un AWS SDK o realizando solicitudes HTTP directamente.

Para eliminar una política de autenticación de remitentes mediante el AWS CLI

- En la línea de comando, escriba el comando siguiente:

```
aws ses delete-identity-policy --identity example.com --policy-name samplePolicy
```

  En este comando, reemplace *ejemplo.com* por la identidad que contiene la política de autenticación de remitente. Reemplace *políticaEjemplo* por el nombre de la política de autenticación de remitente.

Eliminación de datos relacionados con las reglas de recepción

Si utiliza Amazon SES para recibir correo electrónico entrante, puede crear reglas de recepción que se aplican a una o varias identidades (direcciones de correo electrónico o dominios). Estas reglas determinan qué hace Amazon SES con el correo electrónico entrante enviado a las identidades especificadas.

Para eliminar una regla de recepción con la consola de Amazon SES

1. Abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En Email Receiving (Recepción de correo electrónico), elija Rule Sets (Conjuntos de reglas).
3. Si la regla de recepción forma parte del conjunto de reglas activo, elija View Active Rule Set (Ver conjunto de reglas activo). En caso contrario, elija el conjunto de reglas que contiene la regla de recepción que desea eliminar.
4. En la lista de reglas de recepción, elija la regla que desea eliminar.
5. En el menú Acciones, elija Eliminar.
6. En el cuadro de diálogo de confirmación, elija Delete (Eliminar).

Puede utilizar la API de Amazon SES para eliminar reglas de recepción. El siguiente procedimiento utiliza AWS Command Line Interface (AWS CLI) para interactuar con la API de Amazon SES.

También puede interactuar con la API mediante un AWS SDK o realizando solicitudes HTTP directamente.

Para eliminar una regla de recepción mediante el AWS CLI

- En la línea de comando, escriba el comando siguiente:

```
aws ses delete-receipt-rule --rule-set myRuleSet --rule-name myReceiptRule
```

  En este comando, *myRuleSet*sustitúyalo por el nombre del conjunto de reglas de recepción que contiene la regla de recepción. *myReceiptRule*Sustitúyala por el nombre de la regla de recepción que deseas eliminar.

Eliminación de datos relacionados con los filtros de direcciones IP

Si utiliza Amazon SES para recibir correo electrónico entrante, puede crear filtros para aceptar o bloquear de forma explícita los mensajes que se envíen desde determinadas direcciones IP.

Para eliminar un filtro de dirección IP con la consola de Amazon SES

1. Abra la consola de Amazon SES en https://console.aws.amazon.com/ses/.
2. En Email Receiving (Recepción de correo electrónico), elija IP Address Filters (Filtros de direcciones IP).
3. En la lista de filtros de direcciones IP, elija el filtro que desea quitar y, a continuación, haga clic en Delete (Eliminar).

Puede utilizar la API de Amazon SES para eliminar filtros de direcciones IP. El siguiente procedimiento utiliza AWS Command Line Interface (AWS CLI) para interactuar con la API de Amazon SES. También puede interactuar con la API mediante un AWS SDK o realizando solicitudes HTTP directamente.

Para eliminar un filtro de direcciones IP mediante el AWS CLI

- En la línea de comando, escriba el comando siguiente:

```
aws ses delete-receipt-filter --filter-name IPfilter
```

En este comando, reemplace *filtroIP* por el nombre del filtro de direcciones IP que desea eliminar.

Eliminación de datos en plantillas de correo electrónico

Si utiliza plantillas de correo electrónico para el envío de correo electrónico, es posible que esas plantillas puedan contener datos personales, en función de cómo las haya configurado. Por ejemplo, es posible que haya añadido una dirección de correo electrónico a la plantilla con la que los destinatarios podrían ponerse en contacto para obtener más información.

Solo puede eliminar plantillas de correo electrónico mediante la API de Amazon SES.

Para eliminar una plantilla de correo electrónico mediante el AWS CLI

- En la línea de comando, escriba el comando siguiente:

```
aws ses delete-template --template-name sampleTemplate
```

En este comando, reemplace *plantillaEjemplo* por el nombre de la plantilla de correo electrónico que desea eliminar.

Eliminación de datos en plantillas de correo electrónico de verificación personalizadas

Si utiliza plantillas personalizadas para la comprobación de nuevas direcciones de envío de correo electrónico, es posible que esas plantillas puedan contener datos personales, en función de cómo las haya configurado. Por ejemplo, es posible que haya añadido una dirección de correo electrónico a la plantilla de correo electrónico de verificación con la que los destinatarios podrían ponerse en contacto para obtener más información.

Solo puede eliminar plantillas de correo electrónico de verificación personalizado mediante la API de Amazon SES.

Para eliminar una plantilla de correo electrónico de verificación personalizada mediante el AWS CLI

- En la línea de comando, escriba el comando siguiente:

```
aws ses delete-custom-verification-email-template --template-
name verificationEmailTemplate
```

En este comando, *verificationEmailTemplate*sustitúyala por el nombre de la plantilla de correo electrónico de verificación personalizada que deseas eliminar.

Elimine todos los datos personales cerrando su AWS cuenta

También es posible eliminar todos los datos personales almacenados en Amazon SES al cerrar su cuenta de AWS . Sin embargo, esta acción también elimina todos los demás datos, personales o no personales, que haya almacenado en todos los demás servicios. AWS

Al cerrar la AWS cuenta, los datos de la cuenta se conservan durante 90 AWS días. Después de ese periodo de retención, se eliminan de forma permanente e irreversible.

Para cerrar tu AWS cuenta

Las instrucciones completas sobre cómo cerrar tu AWS cuenta se encuentran en Cerrar una AWS cuenta.

Identity and Access Management en Amazon SES

Puede usar AWS Identity and Access Management (IAM) con Amazon Simple Email Service (Amazon SES) para especificar qué acciones de la API de SES puede realizar un usuario, grupo o rol. (En este tema hacemos referencia a estas entidades colectivamente como usuario). También puede controlar qué direcciones de correo electrónico puede utilizar el usuario para las direcciones de remitente ("From"), destinatario y "Return-Path" de los correos electrónicos.

Por ejemplo, puede crear una política de IAM que permita a los usuarios de su organización enviar correos electrónicos, pero no llevar a cabo acciones administrativas tales como estadísticas de envío de comprobación. Otro ejemplo, puede escribir una política que permita a un usuario enviar correos electrónicos a través de SES desde su cuenta, pero solo si utilizan una dirección de remitente ("From") específica.

Para utilizar IAM, defina una política de IAM, que es un documento que define de forma explícita los permisos y adjunta la política a un usuario. Para obtener información sobre cómo crear políticas de IAM, consulte la Guía del usuario de IAM. Aparte de aplicar las restricciones que establezca en su política, no hay cambios en el modo en que los usuarios interactúan con SES o en cómo SES lleva a cabo las solicitudes.

> **Note**
>
> - Si la cuenta está en el entorno aislado de SES, sus restricciones impiden la implementación de algunas de estas políticas; consulte Solicitar acceso de producción.
> - También puede controlar el acceso a SES utilizando políticas de autorización de envío. Mientras que las políticas de IAM restringen lo que pueden hacer los usuarios, las políticas de autorización de envío restringen cómo se pueden utilizar las identidades verificadas. Además, solo las políticas de autorización de envío pueden otorgar acceso entre cuentas. Para obtener más información acerca de la autorización de envío, consulte Uso de la autorización de envío con Amazon SES.

Si busca información sobre cómo generar credenciales de SMTP de SES para un usuario existente, consulte Obtención de las credenciales de SMTP de Amazon SES.

Creación de políticas de IAM para acceso a SES

En esta sección se explica cómo puede utilizar las políticas de IAM; específicamente con SES. Para obtener información sobre cómo crear políticas de IAM en general consulte la Guía del usuario de IAM.

Existen tres razones por las que podría utilizar IAM con SES:

- Para restringir la acción de envío de correo electrónico.
- Para restringir las direcciones "From", de destinatario y de "Return-Path" de los correos electrónicos que el usuario envía.
- Para controlar aspectos generales del uso de la API, como el periodo de tiempo durante el que se permite que un usuario llame a las API que está autorizado a utilizar.

Restringir la acción

Para controlar qué acciones de SES puede realizar un usuario, utilice el elemento `Action` de una política de IAM. Puede establecer el elemento `Action` en cualquier acción de API de SES poniendo como prefijo en el nombre de la API la cadena en minúsculas `ses:`. Por ejemplo, puede establecer `Action` en `ses:SendEmail`, `ses:GetSendStatisticso` `ses:*` (para todas las acciones).

A continuación, en función de `Action`, especifique el elemento `Resource` de la siguiente manera:

Si el elemento **`Action`** solo permite el acceso a API de envío de correo electrónico (es decir, **`ses:SendEmail`** o **`ses:SendRawEmail`**):

- Para permitir que el usuario envíe desde cualquier identidad suya Cuenta de AWS, establézcalo en `Resource` *
- Para restringir las identidades desde las que un usuario puede enviar, establezca `Resource` en los ARN de las identidades que el usuario tiene permiso para utilizar.

Si el elemento **`Action`** permite el acceso a todos los API:

- Si no desea restringir las identidades desde las que puede enviar el usuario, establezca `Resource` en *
- Si desea restringir las identidades desde las que un usuario puede enviar, debe crear dos políticas (o dos instrucciones dentro de una política):
  - Uno que esté `Action` configurado en una lista explícita de las non-email-sending API permitidas y `Resource` establecido en *
  - Una con `Action` establecido en uno de los API de envío de correo electrónico (`ses:SendEmail` o `ses:SendRawEmail`) y `Resource` definido en los ARN de las identidades que permite utilizar al usuario.

Para obtener una lista de acciones de SES disponibles, consulte la Referencia de la API de Amazon Simple Email Service. Si el usuario va a utilizar la interfaz de SMTP, debe permitir como mínimo el acceso a `ses:SendRawEmail`.

Restricción de direcciones de correo electrónico

Si desea restringir al usuario a direcciones de correo electrónico específicas, puede utilizar un bloque `Condition`. En el bloque `Condition`, debe especificar las condiciones utilizando claves de condición tal y como se describe en la Guía del usuario de IAM. Mediante el uso de claves de condición, podrá controlar las siguientes direcciones de correo electrónico:

> **Note**
>
> Estas claves de condición de dirección de correo electrónico se aplican únicamente a los API indicados en la siguiente tabla.

Clave de condición	Descripción	API
`ses:Recipients`	Restringe las direcciones del destinatario, que incluyen las direcciones To:, "CC" y "BCC".	`SendEmail` , `SendRawEmail`
`ses:FromAddress`	Restringe la dirección de remitente ("From").	`SendEmail` , `SendRawEmail` , `SendBounce`
`ses:FromDisplayName`	Restringe la dirección de remitente ("From") que se utiliza como nombre de visualización.	`SendEmail` , `SendRawEmail`
`ses:FeedbackAddress`	Restringe la dirección "Return-Path", que es la dirección donde se pueden enviar los rebotes y las reclamaciones mediante reenvío de retroalimentación de correo electrónico. Para obtener información acerca del reenvío de retroalimentación de correo electrónico, consulte Recepción de notificaciones de Amazon SES por correo electrónico.	`SendEmail` , `SendRawEmail`

Restricción por versión de la API de SES

Mediante el uso de la clave de `ses:ApiVersion` en condiciones, puede restringir el acceso a SES en función de la versión de la API de SES.

> **Note**
>
> La interfaz de SMTP de SES utiliza la API de SES versión 2 de `ses:SendRawEmail`.

Restricción del uso general de la API

Al utilizar claves AWS amplias en determinadas condiciones, puede restringir el acceso a SES en función de aspectos como la fecha y la hora en que el usuario puede acceder a las API. SES implementa solo las siguientes claves AWS de política generales:

- `aws:CurrentTime`
- `aws:EpochTime`
- `aws:SecureTransport`
- `aws:SourceIp`
- `aws:SourceVpc`
- `aws:SourceVpce`
- `aws:UserAgent`
- `aws:VpcSourceIp`

Para obtener más información acerca de estas claves, consulte la Guía del usuario de IAM.

Ejemplos de políticas de IAM para SES

En este tema se ofrecen ejemplos de políticas que permiten a un usuario acceder a SES, pero solo en determinadas condiciones.

Ejemplos de políticas de esta sección:

- Permitir el acceso completo a todas las acciones de SES
- Permitir el acceso solo a la API de SES versión 2
- Permitir el acceso solo a acciones de envío de correo electrónico
- Restricción del periodo de tiempo de envío
- Restricción de las direcciones de destinatario
- Restricción de la dirección de remitente ("From")
- Restricción del nombre de visualización del remitente de correo electrónico
- Restringir el destino de retroalimentación de rebotes y reclamaciones

Permitir el acceso completo a todas las acciones de SES

La siguiente política permite a un usuario llamar a cualquier acción de SES.

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

Permitir el acceso solo a la API de SES versión 2

La siguiente política permite a un usuario llamar solo a las acciones de SES de la API versión 2.

```
{
                    "Version":"2012-10-17",
                    "Statement":[
                        {
                            "Effect":"Allow",
                            "Action":[
                            "ses:*"
                            ],
                            "Resource":"*",
                            "Condition": {
                                "StringEquals" : {
                                "ses:ApiVersion" : "2"
                                }
                            }
                        }
                    ]
                }
```

Permitir el acceso solo a acciones de envío de correo electrónico

La siguiente política permite a un usuario enviar correos electrónicos a través de SES, pero no permite al usuario llevar a cabo acciones administrativas como, por ejemplo, el acceso a las estadísticas de envío de SES.

```
{
```

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

Restricción del periodo de tiempo de envío

La siguiente política permite a un usuario llamar a las API de envío de correo electrónico de SES solo durante el mes de septiembre de 2018.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource":"*",
      "Condition":{
        "DateGreaterThan":{
          "aws:CurrentTime":"2018-08-31T12:00Z"
        },
        "DateLessThan":{
          "aws:CurrentTime":"2018-10-01T12:00Z"
        }
      }
    }
  ]
}
```

Restricción de las direcciones de destinatario

La siguiente política permite a un usuario llamar a las API de envío de correo electrónico de SES, pero solo a las direcciones de los destinatarios que pertenezcan al dominio example.com (`StringLike` distingue entre mayúsculas y minúsculas).

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource":"*",
      "Condition":{
        "ForAllValues:StringLike":{
          "ses:Recipients":[
            "*@example.com"
          ]
        }
      }
    }
  ]
}
```

Restricción de la dirección de remitente ("From")

La siguiente política permite a un usuario llamar a las API de envío de correo electrónico de SES, pero solo si la dirección de remitente ("From") es marketing@example.com.

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

```
      "Condition":{
        "StringEquals":{
          "ses:FromAddress":"marketing@example.com"
        }
      }
    }
  ]
}
```

La siguiente política permite a un usuario llamar a la SendBounceAPI, pero solo si la dirección «De» es bounce@example.com.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendBounce"
      ],
      "Resource":"*",
      "Condition":{
        "StringEquals":{
          "ses:FromAddress":"bounce@example.com"
        }
      }
    }
  ]
}
```

Restricción del nombre de visualización del remitente de correo electrónico

La siguiente política permite a un usuario llamar a las API de envío de correo electrónico de SES, pero solo si el nombre de visualización de la dirección del remitente "From" incluye Marketing (`StringLike` distingue entre mayúsculas y minúsculas).

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
```

```
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource":"*",
      "Condition":{
        "StringLike":{
          "ses:FromDisplayName":"Marketing"
        }
      }
    }
  ]
}
```

Restringir el destino de retroalimentación de rebotes y reclamaciones

La siguiente política permite a un usuario llamar a las API de envío de correo electrónico de SES, pero solo si la dirección “Ruta de devolución” del correo electrónico se ha establecido en feedback@example.com.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource":"*",
      "Condition":{
        "StringEquals":{
          "ses:FeedbackAddress":"feedback@example.com"
        }
      }
    }
  ]
}
```

AWS políticas gestionadas para Amazon Simple Email Service

Para añadir permisos a usuarios, grupos y roles, es más fácil usar políticas AWS administradas que escribirlas usted mismo. Se necesita tiempo y experiencia para crear políticas administradas

por el cliente de IAM que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puedes usar nuestras políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en tu AWS cuenta. Para obtener más información sobre las políticas AWS administradas, consulte las políticas AWS administradas en la Guía del usuario de IAM.

AWS los servicios mantienen y AWS actualizan las políticas gestionadas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios añaden permisos adicionales a una política AWS gestionada para admitir nuevas funciones. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Lo más probable es que los servicios actualicen una política AWS administrada cuando se lanza una nueva función o cuando hay nuevas operaciones disponibles. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política ReadOnlyAccess AWS gestionada proporciona acceso de solo lectura a todos los AWS servicios y recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

AWS política gestionada: AmazonSES FullAccess

Puede adjuntar la política `AmazonSESFullAccess` a las identidades de IAM. Proporciona acceso completo a Amazon SES.

Para ver los permisos de esta política, consulte AmazonSES FullAccess en la Referencia de políticas AWS gestionadas.

AWS política gestionada: AmazonSES ReadOnlyAccess

Puede adjuntar la política `AmazonSESReadOnlyAccess` a las identidades de IAM. Proporciona acceso de solo lectura a Amazon SES.

Para ver los permisos de esta política, consulte AmazonSES ReadOnlyAccess en la Referencia de políticas AWS administradas.

AWS política gestionada: AmazonSES ServiceRolePolicy

No puede adjuntar la política `AmazonSESServiceRolePolicy` a sus entidades de IAM. Esta política se adjunta a una función vinculada al servicio que permite a Amazon SES realizar acciones

en su nombre. Para obtener más información, consulte Permisos de roles vinculados a servicios para Amazon SES.

Para ver los permisos de esta política, consulte AmazonSES ServiceRolePolicy en la referencia de políticas AWS gestionadas.

Amazon Simple Email Service actualiza las políticas AWS gestionadas

Consulta los detalles y las actualizaciones de las políticas AWS gestionadas de Amazon Simple Email Service desde que este servicio comenzó a rastrear estos cambios.

Cambio	Descripción	Fecha
Amazon Simple Email Service agregó una nueva política de administración	Amazon Simple Email Service se agregó `AmazonSES ServiceRolePolicy` a la función vinculada al servicio `AWSServiceRoleForA mazonSES` que permite a SES realizar acciones en su nombre	13 de mayo de 2024
Amazon Simple Email Service actualizó una definición de política	Amazon Simple Email Service aclaró que la entrada anterior de esta tabla (fila inferior) decía: Amazon Simple Email Service se agregó `ses:Batch GetMetricData` a la política ReadOnlyAccess administrada de AmazonSE; esto dará acceso a la API de SES. BatchGetMetricData	30 de abril de 2024
Amazon Simple Email Service actualizó una definición de política	Se agregó Amazon Simple Email Service `ses:Batch Get*` a la política ReadOnlyAccess gestionad	16 de febrero de 2024

Cambio	Descripción	Fecha
	a de AmazonSE, lo que dará acceso a la API de SES. BatchGetMetricData	
Amazon Simple Email Service ha cambiado dos definiciones de políticas	Amazon Simple Email Service ha eliminado «a través AWS de la consola de administración» del final de las definiciones de AmazonSES FullAccess y ReadOnlyAccess AmazonSES.	3 de mayo de 2023
Amazon Simple Email Service comenzó a realizar un seguimiento de los cambios	Amazon Simple Email Service comenzó a rastrear los cambios en sus políticas AWS gestionadas	5 de abril de 2023

Uso de funciones vinculadas a servicios para Amazon SES

Amazon Simple Email Service (SES) AWS Identity and Access Management utiliza funciones vinculadas al servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Amazon SES. SES predefine las funciones vinculadas al servicio e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración de SES, ya que no es necesario añadir manualmente los permisos necesarios. SES define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo SES puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. Esto protege sus recursos de SES porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna

Roles vinculados a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios para Amazon SES

SES usa el rol vinculado al servicio denominado AWSServiceRoleForAmazonSES: Permite a SES publicar las métricas de monitoreo CloudWatch básicas de Amazon en nombre de sus recursos de SES.

El rol AWSServiceRoleForAmazonSES vinculado al servicio confía en que el siguiente servicio asuma el rol:

- `ses.amazonaws.com`

La política de permisos de roles denominada AmazonSES ServiceRolePolicy es una política AWS administrada que permite a SES realizar las siguientes acciones en los recursos especificados:

- Acción: `cloudwatch:PutMetricData` en el espacio de nombres `AWS/SES` CloudWatch. Esta acción otorga permiso a SES para colocar datos métricos en el espacio de CloudWatch `AWS/SES` nombres. Para obtener más información sobre las métricas de SES disponibles en CloudWatch, consulte. Registro y monitoreo en Amazon SES
- Acción: `cloudwatch:PutMetricData` en el espacio de nombres `AWS/SES/MailManager` CloudWatch . Esta acción otorga permiso a SES para colocar datos de métricas en el espacio de CloudWatch `AWS/SES/MailManager` nombres. Para obtener más información sobre las métricas de SES disponibles en CloudWatch, consulte. Registro y monitoreo en Amazon SES
- Acción: `cloudwatch:PutMetricData` en el espacio de nombres `AWS/SES/Addons` CloudWatch . Esta acción otorga permiso a SES para colocar datos de métricas en el espacio de CloudWatch `AWS/SES/Addons` nombres. Para obtener más información sobre las métricas de SES disponibles en CloudWatch, consulte. Registro y monitoreo en Amazon SES

Debe configurar los permisos para permitir a sus usuarios, grupos o funciones, crear, editar o eliminar la descripción de un rol vinculado al servicio. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio para Amazon SES

No necesita crear manualmente un rol vinculado a servicios. Al crear recursos de SES en la AWS Management Console, la o la AWS API AWS CLI, SES crea automáticamente la función vinculada al servicio.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear recursos de SES, SES vuelve a crear el rol vinculado al servicio para usted.

Edición de un rol vinculado a un servicio para Amazon SES

SES no le permite editar el rol vinculado al AWSServiceRoleForAmazonSES servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM.

Eliminar un rol vinculado a un servicio para SES

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma, no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe limpiar el rol vinculado a servicios antes de eliminarlo manualmente.

Limpiar un rol vinculado a un servicio

Antes de poder usar IAM para eliminar un rol vinculado a un servicio, primero debe eliminar todos los recursos de SES.

> **Note**
>
> Si el servicio SES utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Eliminar manualmente el rol vinculado al servicio

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSServiceRoleForAmazonSES servicio. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones compatibles para las funciones vinculadas al servicio de Amazon SES

SES no admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio está disponible. Puede usar el AWSServiceRoleForAmazonSES rol en las siguientes regiones.

Nombres de las regiones	Identidad de la región	Support in SES
Este de EE. UU. (Norte de Virginia)	us-east-1	Sí
Este de EE. UU. (Ohio)	us-east-2	Sí
Asia Pacífico (Sídney)	ap-southeast-2	Sí
Asia Pacífico (Tokio)	ap-northeast-1	Sí
Europa (Frankfurt)	eu-central-1	Sí
Europa (Irlanda)	eu-west-1	Sí

Registro y monitoreo en Amazon SES

El monitoreo es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon SES y las soluciones de AWS. AWS brinda herramientas para ayudarlo a monitorear Amazon SES y responder a incidentes potenciales.

- Amazon CloudWatch monitorea los recursos de AWS y las aplicaciones que ejecuta en AWS en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Para obtener más información, consulte Recuperación de datos de eventos de Amazon SES desde CloudWatch y Creación de alarmas de monitoreo de reputación en CloudWatch.
- AWS CloudTrail captura las llamadas a la API y otros eventos relacionados que realiza la Cuenta de AWS o se realizan en nombre de esta. Además, entrega los archivos de registros a un bucket de Amazon S3 especificado. También pueden identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que se hicieron. Para obtener más información, consulte Registro de llamadas a la API de Amazon SES con AWS CloudTrail.
- Los eventos de envío de correo electrónico de Amazon SES pueden ayudarle a ajustar su estrategia de envío de correo electrónico. Amazon SES captura información detallada, incluidos

los números de envíos, entregas, aperturas, clics, rebotes, reclamos y rechazos. Para obtener más información, consulte Monitoreo de la actividad de envío.

- Las métricas de reputación de Amazon SES realizan un seguimiento de las tasas de rebotes y reclamos de su cuenta. Para obtener más información, consulte Monitoreo de su reputación de remitente.

Registro de llamadas a la API de Amazon SES con AWS CloudTrail

Amazon SES se integra con AWS CloudTrail, un servicio que proporciona un registro de las medidas adoptadas por un usuario, un rol o un servicio de AWS en Amazon SES. CloudTrail captura las llamadas a la API de Amazon SES como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de Amazon SES y las llamadas desde el código a las operaciones de la API de Amazon SES. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos de Amazon SES. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Event history (Historial de eventos). Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Amazon SES, la dirección IP desde la que se realizó la solicitud, quién realizó la solicitud, cuándo se realizó y otros detalles adicionales.

Para obtener más información acerca de CloudTrail, incluso cómo configurarlo y habilitarlo, consulte la Guía del usuario de AWS CloudTrail.

Información de Amazon SES en CloudTrail

CloudTrail se habilita en su Cuenta de AWS cuando la crea. Cuando se produce una actividad de eventos compatible en Amazon SES, la actividad se registra en un evento de CloudTrail junto con otros eventos de servicios de AWS en Event history (Historial de eventos). Puede ver, buscar y descargar los últimos eventos de la Cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de los eventos de la Cuenta de AWS, incluidos los eventos de Amazon SES, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos

recopilados en los registros de CloudTrail. Para obtener más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de registro de CloudTrail de varias regiones y Recibir archivos de registro de CloudTrail de varias cuentas

Amazon SES admite el registro de todas las acciones enumeradas en Referencia de la API de SES y Referencia de la API de SES v2 como eventos en archivos de registro de CloudTrail:

> **Note**
>
> Amazon SES entrega eventos de administración a CloudTrail. Los eventos de administración incluyen acciones relacionadas con la creación y administración de recursos de su Cuenta de AWS. En Amazon SES, los eventos de administración incluyen acciones como la creación y eliminación de identidades o reglas de recepción.
> Los eventos de administración son distintos de los eventos de datos. Los eventos de datos son eventos relacionados con el acceso a los datos y la interacción con estos en su Cuenta de AWS. En Amazon SES, los eventos de datos incluyen acciones tales como el envío de mensajes de correo electrónico.
> Dado que Amazon SES solo proporciona eventos de administración a CloudTrail, los siguientes eventos no se registran en CloudTrail:
>
> - SendEmail
> - SendRawEmail
> - SendTemplatedEmail
> - SendBulkTemplatedEmail
>
> Puede utilizar la publicación de eventos para registrar eventos relacionados con el envío de correo electrónico. Para obtener más información, consulte Monitoreo del envío de correo electrónico mediante la publicación de eventos de Amazon SES.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario AWS Identity and Access Management (IAM) o credenciales de usuario raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte el Elemento userIdentity de CloudTrail.

Ejemplo: Entradas del archivo de registros de Amazon SES

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

En el ejemplo siguiente, se muestra una entrada de registro de CloudTrail que ilustra las acciones `DeleteIdentity` y `VerifyEmailIdentity`.


```
{
  "Records":[
    {
      "awsRegion":"us-west-2",
      "eventID":"0ffa308d-1467-4259-8be3-c749753be325",
      "eventName":"DeleteIdentity",
      "eventSource":"ses.amazonaws.com",
      "eventTime":"2018-02-02T21:34:50Z",
      "eventType":"AwsApiCall",
      "eventVersion":"1.02",
      "recipientAccountId":"111122223333",
      "requestID":"50b87bfe-ab23-11e4-9106-5b36376f9d12",
      "requestParameters":{
        "identity":"amazon.com"
      },
      "responseElements":null,
      "sourceIPAddress":"192.0.2.0",
```

```
      "userAgent":"aws-sdk-java/unknown-version",
      "userIdentity":{
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "accountId":"111122223333",
        "arn":"arn:aws:iam::111122223333:root",
        "principalId":"111122223333",
        "type":"Root"
      }
    },
    {
      "awsRegion":"us-west-2",
      "eventID":"5613b0ff-d6c6-4526-9b53-a603a9231725",
      "eventName":"VerifyEmailIdentity",
      "eventSource":"ses.amazonaws.com",
      "eventTime":"2018-02-04T01:05:33Z",
      "eventType":"AwsApiCall",
      "eventVersion":"1.02",
      "recipientAccountId":"111122223333",
      "requestID":"eb2ff803-ac09-11e4-8ff5-a56a3119e253",
      "requestParameters":{
        "emailAddress":"sender@example.com"
      },
      "responseElements":null,
      "sourceIPAddress":"192.0.2.0",
      "userAgent":"aws-sdk-java/unknown-version",
      "userIdentity":{
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "accountId":"111122223333",
        "arn":"arn:aws:iam::111122223333:root",
        "principalId":"111122223333",
        "type":"Root"
      }
    }
  ]
}
```

Validación de conformidad para Amazon Simple Email Service

Auditores externos evalúan la seguridad y la conformidad de Amazon Simple Email Service como parte de varios programas de conformidad de AWS. Estos incluyen SOC, PCI, FedRAMP, HIPAA y otros.

Para obtener una lista de los servicios de AWS en el ámbito de programas de conformidad específicos, consulte AWS Services in Scope by Compliance Program (Servicios en el ámbito de programas de conformidad). Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

Su responsabilidad en cuanto a conformidad al usar Amazon Simple Email Service está determinada por la confidencialidad de sus datos, los objetivos de conformidad de su compañía y las leyes y regulaciones aplicables. AWS proporciona los siguientes recursos para ayudarle con la conformidad:

- Security and Compliance Quick Start Guides (Guías de inicio rápido de seguridad y conformidad) (Guías de inicio rápido de seguridad y conformidad): Estas guías de implementación analizan consideraciones sobre arquitectura y proporcionan los pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Documento técnico sobre arquitectura para seguridad y conformidad de HIPAA : en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones conformes con HIPAA.
- AWSRecursos de conformidad de: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config: AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este servicio de AWS proporciona una vista integral de su estado de seguridad en AWS que lo ayuda a verificar la conformidad con los estándares y las prácticas recomendadas del sector de seguridad.

Resiliencia de Amazon Simple Email Service

La infraestructura global de AWS está conformada por regiones y zonas de disponibilidad de AWS. Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre zonas de disponibilidad y las regiones de AWS, consulte Infraestructura global de AWS.

Seguridad de la infraestructura en Amazon Simple Email Service

Como se trata de un servicio administrado, Amazon Simple Email Service está protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y cómo AWS protege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS con las prácticas recomendadas de seguridad de infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Puede utilizar llamadas a la API publicadas en AWS para acceder a Amazon Simple Email Service a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Nosotros exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) tales como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Configuración de puntos de enlace de la VPC con Amazon SES

Muchos clientes de Amazon SES disponen de políticas corporativas que limitan la capacidad de sus sistemas internos para conectarse a la red pública de Internet. Estas políticas impiden el uso de los puntos de conexión de Amazon SES públicos.

Si tiene políticas similares, puede trabajar dentro de estas restricciones mediante Amazon Virtual Private Cloud. Con Amazon VPC, puede implementar AWS recursos en una red virtual que existe en un área aislada del. Nube de AWS Para obtener más información sobre Amazon VPC, consulte la Guía del usuario de Amazon VPC.

Puede conectarse directamente de Amazon VPC a SES a través de un punto de conexión de VPC de forma segura y escalable. Cuando utiliza un punto de conexión de VPC de interfaz, ofrece una

mejor postura de seguridad, ya que no necesita abrir firewalls de tráfico saliente, además de ofrecer otros beneficios del uso de puntos de conexión de Amazon VPC.

Cuando se utiliza un punto de conexión de VPC, el tráfico a SES no se transmite a través de Internet y nunca sale de la red de Amazon para conectar de forma segura la VPC a SES sin riesgos de disponibilidad ni restricciones de ancho de banda en el tráfico de red. Puede centralizar SES en toda la infraestructura de varias cuentas y proporcionarlo como un servicio a las cuentas sin necesidad de utilizar una puerta de enlace de Internet.

Limitaciones

- SES no admite puntos de conexión de VPC en las siguientes zonas de disponibilidad: `use1-az2`, `use1-az3`, `use1-az5`, `usw1-az2`, `usw2-az4`, `apne2-az4`, `cac1-az3` y `cac1-az4`.
- El punto de conexión SMTP utilizado en la VPC está restringido a la Región de AWS que se está utilizando actualmente para la cuenta.

Ejemplo del tutorial de configuración de SES en Amazon VPC

Requisitos previos

Antes de completar el procedimiento de esta sección, debe realizar los pasos que se describen a continuación:

- Tenga una nube privada virtual (VPC) existente o cree una nueva VPC. Para obtener información acerca de los procedimientos, consulte Comenzar a utilizar Amazon VPC.
- Lance una instancia de Amazon EC2 en la VPC para probar la conectividad con el punto de conexión de VPC creado en un paso posterior. Para obtener más información, consulte VPC predeterminadas.

Note

Si bien los puntos de conexión de VPC para SES se pueden usar con cualquier recurso, para facilitar el método de prueba, en este ejemplo se utilizará una instancia EC2 como recurso. Dado que Amazon EC2 restringe el tráfico de correo electrónico a través del

puerto 25 de forma predeterminada, tendrá que usar un puerto diferente al TCP 25, como TCP 465, 587, 2465 o 2587.

Configuración de SES en Amazon VPC

El proceso de configuración de un punto de conexión de VPC que se va a utilizar con SES consta de unos pocos pasos independientes. Primero, debe crear un grupo de seguridad que permita a la instancia comunicarse con los puertos SMTP, luego crear un punto de conexión de VPC para Amazon SES y, por último, probar la conexión con el punto de conexión de VPC para asegurarse de que está configurado correctamente.

Paso 1: Crear el grupo de seguridad

En este paso, se crea un grupo de seguridad que permite a las instancias de Amazon EC2 comunicarse con el punto de conexión de interfaz de VPC que creará.

Para crear el grupo de seguridad

1. En el panel de navegación de la consola de Amazon EC2, en Network & Security (Seguridad y redes), elija Security Groups (Grupos de seguridad).
2. Elija Crear grupo de seguridad.
3. En Basic details (Detalles básicos), haga lo siguiente:
   - En Security group name (Nombre de grupo de seguridad), escriba un nombre único que identifique el grupo de seguridad.
   - En Description (Descripción), puede especificar texto que describa el objetivo del grupo de seguridad.
   - En VPC elija la VPC en la que desea utilizar Amazon SES.
4. En Inbound rules (Reglas de entrada), elija Add rule (Agregar regla).
5. Para la nueva Regla de entrada, haga lo siguiente:
   - En Type (Tipo), elija Custom TCP (TCP personalizada).
   - En Port range (Intervalo de puertos), introduzca el número de puerto que desea utilizar para enviar correo electrónico. Puede utilizar cualquiera de los siguientes números de puerto: **465**, **587**, **2465** o **2587**.
   - En Source type (Tipo de origen), elija Custom (Personalizado).

- Para Fuente, escriba el rango de IP CIDR privado u otros ID de grupo de seguridad que contengan los recursos que usará el punto de conexión de VPC para comunicarse con el servicio de SES.
- (Repita los pasos 4 y 5 para cada rango de CIDR o grupo de seguridad desde el que desee permitir el acceso).

6. Cuando termine, elija Create security group (Crear grupo de seguridad).

Paso 2: Crear el punto de conexión de VPC

En Amazon VPC, un punto de enlace de VPC le permite conectar su VPC a los servicios compatibles. AWS En este ejemplo, se configura Amazon VPC para que el grupo de seguridad de Amazon EC2 se pueda conectar a Amazon SES.

Para crear el punto de enlace de la VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En Virtual Private Cloud (Nube virtual privada), seleccione Endpoints (Puntos de enlace).
3. Elija Create Endpoint (Crear punto de conexión) para abrir la página Create Endpoint (Crear punto de conexión).
4. (Opcional) En el panel Endpoint settings (Configuración de punto de conexión), cree una etiqueta en el campo Name tag (Etiqueta de nombre).
5. En Categoría de servicio, seleccione Servicios de AWS .
6. En el panel Services (Servicios), filtre por smtp en la barra de búsqueda y, a continuación, seleccione el botón de opción.
7. En el panel VPC, haga clic en la barra de búsqueda y seleccione una VPC del cuadro de la lista (consulte the section called “Requisitos previos”).
8. En el panel Subnets (Subredes), seleccione Availability Zones (Zonas de disponibilidad) y Subnet IDs (ID de subred).

> **Note**
>
> Amazon SES no admite puntos de conexión de VPC en las siguientes Zonas de disponibilidad: `use1-az2`, `use1-az3`, `use1-az5`, `usw1-az2`, `usw2-az4`, `apne2-az4`, `cac1-az3` y `cac1-az4`.

9. En el panel Security groups (Grupos de seguridad), seleccione el grupo de seguridad que creó anteriormente.
10. (Opcional) En el panel Etiquetas, puede crear una o más etiquetas.
11. Seleccione Crear punto de conexión. Espere aproximadamente 5 minutos mientras Amazon VPC crea el punto de enlace. Cuando el punto de conexión esté listo para usar, el valor de la columna Status (Estado) cambia a Available (Disponible).

(Opcional) Paso 3: Probar la conexión al punto de conexión de VPC

Cuando complete el proceso de configuración del punto de conexión de VPC, puede probar la conexión para asegurarse de que el punto de conexión de VPC esté configurado correctamente. Puede probar la conexión mediante herramientas de la línea de comandos que se incluyen con la mayoría de los sistemas operativos.

Para probar la conexión con el punto de enlace de la VPC

1. Lance una instancia de Amazon EC2 en la misma VPC donde acaba de crear el punto de conexión de VPC email-smtp.

   Para obtener información sobre la conexión a instancias de Linux, consulte Conectarse a su instancia de Linux en la Guía del usuario de Amazon EC2.

   Para obtener información sobre la conexión a instancias de Windows, consulte el tutorial de introducción de la Guía del usuario de Amazon EC2.
2. Envíe un correo electrónico de prueba, por ejemplo, mediante la interfaz de SMTP de SES.

> **Note**
>
> Deberá verificar una dirección de correo electrónico o un dominio para poder enviar mensajes de correo electrónico a través de Amazon SES. Para obtener más información sobre la verificación de identidades, consulte Creación y verificación de identidades en Amazon SES.

Solución de problemas de Amazon SES

Esta sección contiene los siguientes temas que podrían ayudarle cuando encuentre problemas:

- Para obtener información sobre los problemas de verificación de dominio que podría encontrarse, consulte Problemas de verificación de dirección de correo electrónico y dominios.
- Para obtener soluciones a problemas relacionados con DKIM, consulte Solución de problemas de DKIM en Amazon SES.
- Para obtener una lista de problemas de entrega comunes que podría encontrar al enviar correo electrónico, junto con las medidas correctivas que puede tomar, consulte Problemas de entrega de Amazon SES.
- Para obtener una descripción de los problemas que los destinatarios podrían encontrar al recibir un correo electrónico que se envió a través de Amazon SES, consulte Problemas con correos electrónicos recibidos de Amazon SES.
- Para soluciones de problemas con notificaciones de rebotes, reclamaciones y entregas, consulte Problemas de notificaciones de Amazon SES.
- Para ver una lista de los errores que pueden producirse al enviar un correo electrónico con Amazon SES, consulte Errores de envío de correo electrónico de Amazon SES.
- Para obtener sugerencias sobre cómo aumentar la velocidad de envío de correo electrónico al realizar varias llamadas a Amazon SES mediante la API o la interfaz de SMTP, consulte Aumento del rendimiento con Amazon SES.
- Para obtener soluciones a problemas comunes que pueden aparecer al utilizar Amazon SES a través de su interfaz Simple Mail Transfer Protocol (SMTP), así como una lista de códigos de respuesta SMTP devueltos por Amazon SES, consulte Problemas de SMTP de Amazon SES.
- Para obtener una lista de códigos de error comunes devueltos por la API de Amazon SES v2, consulteErrores comunes.
- Para obtener una descripción de los problemas comunes relacionados con nuestro proceso de revisión de envíos y cómo solucionarlos, consulte Preguntas frecuentes acerca del proceso de revisión de envío de Amazon SES.
- Para obtener información acerca de cómo afectan a su envío con Amazon SES las listas de agujero negro basadas en DNS (DNSBL), consulte Preguntas frecuentes acerca de la lista de agujeros negros de DNS (DNSBL).

Si llama a la API de Amazon SES directamente, consulte la Referencia de la API de Amazon Simple Email Service para ver los errores de HTTP que podría recibir.

> **Note**
>
> Si necesita solicitar asistencia técnica, no utilice el enlace de comentarios de las páginas de esta guía para desarrolladores, ya que el formulario lo recibe el equipo de Documentación de AWS, no el Asistencia de AWS. En su lugar, en la página Contacto, explore las diferentes opciones de asistencia disponibles.

Contenido

- Problemas generales de Amazon SES
- Problemas de verificación de dirección de correo electrónico y dominios
- Solución de problemas de DKIM en Amazon SES
- Problemas de entrega de Amazon SES
- Problemas con correos electrónicos recibidos de Amazon SES
- Problemas de notificaciones de Amazon SES
- Errores de envío de correo electrónico de Amazon SES
- Aumento del rendimiento con Amazon SES
- Problemas de SMTP de Amazon SES

Problemas generales de Amazon SES

La información de esta página explicará y ayudará a diagnosticar los problemas que pueda experimentar al utilizar Amazon SES.

Los cambios que realizo no son visibles de inmediato

Al ser un servicio al que se accede a través de equipos de centros de datos de todo el mundo, Amazon SES utiliza un modelo de informática distribuida denominado consistencia final. Cualquier cambio que realice en Amazon SES (o en otros servicios de AWS) tardará en aparecer en todos los puntos de enlace posibles. Este retraso se debe en parte al tiempo que se tarda en enviar los datos de un servidor a otro y entre regiones de todo el mundo. En la mayoría de los casos, este retraso no durará más de unos minutos.

Algunos ámbitos en los que podría observar un retraso incluyen:

- Creación y modificación de conjuntos de configuración: al crear o modificar un conjunto de configuración (por ejemplo, si se asocia un grupo de IP dedicadas con una configuración existente), es posible que haya un breve retraso desde el momento en que se crea o modifica hasta el momento en que dichos cambios están activos.
- Creación y modificación de destinos de eventos: al crear o modificar un destino de evento (por ejemplo, para indicar a Amazon SES que envíe sus datos de envío de correo electrónico a otro servicio de AWS), podría haber un retraso entre el momento en que crea o modifica el destino de eventos y el momento en que los eventos de envío de correo electrónico llegan al destino especificado.

Problemas de verificación de dirección de correo electrónico y dominios

Para verificar un dominio o una dirección de correo electrónico con Amazon SES, inicie el proceso utilizando la consola de Amazon SES o la API de Amazon SES. Esta sección contiene información que podría ayudarle a resolver problemas con el proceso de verificación.

> **Note**
>
> En los siguientes procedimientos, la referencia a los registros DNS podría hacer referencia a registros CNAME o TXT según la forma de DKIM que haya utilizado. Easy DKIM utiliza registros CNAME y Utilice su propio DKIM (BYODKIM) utiliza registros TXT. Se proporcionan procedimientos de verificación detallados para cada uno de los Easy DKIM o BYODKIM.

Problemas comunes de verificación de dominio

Si intenta verificar un dominio mediante el procedimiento indicado en the section called “Verificación de una identidad de dominio” y encuentra problemas, revise las causas posibles y las soluciones que aparecen a continuación.

- Está intentando verificar un dominio que no le pertenece: no puede verificar un dominio que no le pertenece. Por ejemplo, si desea enviar correo electrónico a través de Amazon SES desde una dirección del dominio gmail.com, tiene que verificar dicha dirección de correo electrónico específicamente. No se puede verificar todo el dominio gmail.com.

- Está intentando verificar un dominio privado. No se puede verificar un dominio si los registros DNS no se pueden resolver a través del DNS público.
- El proveedor de DNS no permite utilizar guiones bajos en los nombres de registro de DNS: algunos proveedores de DNS no le permiten incluir guiones bajos (_) en los nombres de registro. Sin embargo, el guion bajo el nombre de registro de DKIM es obligatorio. Si su proveedor de DNS no le permite introducir un guion bajo en el nombre del registro, póngase en contacto con el equipo de atención al cliente del proveedor para obtener ayuda.
- El proveedor de DNS ha agregado el nombre de dominio al final del registro de DNS: algunos proveedores de DNS agregan automáticamente el nombre del dominio al nombre de atributo del registro de DNS. Por ejemplo, si crea un registro cuyo nombre de atributo es _domainkey.example.com, es posible que el proveedor añada el nombre de dominio, lo que se traduce en _domainkey.example.com.example.com). Para evitar la duplicación del nombre de dominio, agregue un punto al final del nombre de dominio cuando ingrese el registro de DNS. Este paso indica al proveedor de DNS que no es necesario añadir el nombre de dominio al registro.
- El proveedor de DNS modificó el valor del registro de DNS: algunos proveedores modifican automáticamente los valores del registro de DNS para utilizar solo letras minúsculas. Amazon SES solo verifica su dominio cuando detecta un registro de verificación cuyo valor de atributo coincide exactamente con el valor que Amazon SES proporcionó cuando se inició el proceso de verificación del dominio. Si el proveedor de DNS del dominio cambia los valores de registro de DNS para utilizar solo letras minúsculas, contacte con el proveedor de DNS para obtener ayuda.
- Desea verificar el mismo dominio varias veces: es posible que tenga que verificar un dominio más de una vez porque está enviando desde regiones distintas o porque utiliza el mismo dominio para enviar desde varias cuentas de AWS. Si el proveedor de DNS no le permite tener más de un registro de DNS con el mismo nombre de atributo, es posible que todavía pueda verificar dos dominios. Si el proveedor de DNS lo permite, puede asignar varios valores de atributo al mismo registro de DNS. Por ejemplo, si Amazon Route 53 administra DNS, puede configurar varios valores para el mismo registro CNAME mediante los siguientes pasos:

  1. En la consola de Route 53, elija el registro CNAME que creó cuando verificó el dominio en la primera región.
  2. En el cuadro Value (Valor), vaya hasta el final del valor de atributo existente y, a continuación, pulse Intro.
  3. Añada el valor de atributo para la región adicional y, a continuación, guarde el conjunto de registros.

Si el proveedor de DNS no le permite asignar varios valores al mismo registro de DNS, puede verificar el dominio una vez con _domainkey en el nombre de atributo del registro de DNS y otra vez sin _domainkey en el nombre de atributo. La desventaja de esta solución es que solo puede verificar el mismo dominio dos veces.

Comprobación de la configuración de verificación de dominio

Puede verificar que el registro de DNS de verificación del dominio de Amazon SES se publique correctamente en el servidor DNS utilizando el siguiente procedimiento. Este procedimiento utiliza la herramienta nslookup, que está disponible para Windows y Linux. En Linux, también puede utilizar dig.

Los comandos de estas instrucciones se ejecutaron en Windows 7 y el dominio de ejemplo que utilizamos es ses-example.com configurado con Easy DKIM que usa registros CNAME.

En este procedimiento, primero encuentre los servidores DNS que sirven al dominio y, a continuación, consulte esos servidores para ver los registros CNAME. Usted consulta los servidores DNS que sirven a su dominio porque dichos servidores contienen la información más actualizada para su dominio, que puede tardar tiempo en propagarse a otros servidores de DNS.

Para verificar que los registros CNAME de verificación de dominio se publican en el servidor DNS

1. Encuentre los servidores de nombres de su dominio siguiendo estos pasos.

    a. Vaya a la línea de comando. Para acceder a la línea de comando en Windows 7, elija Start y, a continuación, escriba cmd. En los sistemas operativos basados en Linux, abra una ventana de terminal.

    b. En el símbolo del sistema, escriba lo siguiente, donde <domain> es el dominio. Esto mostrará un listado de todos los nombres de servidor que sirven a su dominio.

    ```
    nslookup -type=NS <domain>
    ```

    Si su dominio fuera ses-example.com, este comando tendría el siguiente aspecto:

    ```
    nslookup -type=NS ses-example.com
    ```

La salida del comando enumerará los servidores de nombre que sirven a su dominio. Consultará a uno de estos servidores en el siguiente paso.

2. Verifique que los registros CNAME se han publicado correctamente siguiendo estos pasos. Tenga en cuenta que Amazon SES genera tres registros CNAME para la autenticación de Easy DKIM, así que repita los siguientes procedimientos para cada uno de los tres.

   a. En el símbolo del sistema, escriba lo siguiente, donde **<cadena aleatoria>** es el nombre de CNAME generado por SES, **<dominio>** y **<servidor de nombres>** es uno de los servidores de nombres que encontró en el paso 1.

   ```
   nslookup -type=CNAME <random string>_domainkey.<domain> <name server>
   ```

   En nuestro ejemplo ses-example.com, si un servidor de nombres que encontramos en el paso 1 se llamara ns1.name-server.net y **<cadena aleatoria>** generada por SES es `4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz`, escribiríamos lo siguiente:

   ```
   nslookup -type=CNAME 4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz_domainkey.ses-example.com
    ns1.name-server.net
   ```

   b. En la salida del comando, verifique que la cadena que sigue a `canonical name =` coincide con el valor de CNAME que ve a la hora de elegir el dominio en la lista de identidades de la consola de Amazon SES.

   En nuestro ejemplo, buscamos un registro CNAME en `4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz_domainkey.ses-example.com` con un valor de `4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz.dkim.amazonses.com`. Si el registro está publicado correctamente, esperaríamos que el comando tuviera la siguiente salida:

   ```
   4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz_domainkey.ses-example.com canonical name =
    "4hzwn5lmznmmjyl2pqf2agr3uzzzzxyz.dkim.amazonses.com"
   ```

Problemas comunes de verificación de correo electrónico

- El correo electrónico de verificación no llegó: si completa los procedimientos de Verificación de una identidad de dirección de correo electrónico pero no recibe el correo electrónico de verificación en el plazo de unos minutos, siga los pasos que se describen a continuación.

- Compruebe la carpeta de correo no deseado o spam de la dirección de correo electrónico que está intentando verificar.
- Confirme que la dirección que intenta verificar es capaz de recibir correo electrónico. Utilice una dirección de correo electrónico independiente (como, por ejemplo, su dirección de correo electrónico personal) para enviar un correo electrónico de prueba a la dirección que desea verificar.
- Consulte la lista de direcciones verificadas en la consola de Amazon SES. Asegúrese de que no hay ningún error en la dirección de correo electrónico que está intentando verificar.

Solución de problemas de DKIM en Amazon SES

En esta sección se enumeran algunos de los problemas que puede encontrar al configurar la autenticación de DKIM en Amazon SES. Si intenta configurar DKIM y encuentra problemas, revise las posibles causas y las soluciones que aparecen a continuación.

Ha configurado DKIM correctamente, pero sus mensajes no están firmados por DKIM

Si ha utilizado Easy DKIM o BYODKIM para configurar DKIM para un dominio, pero los mensajes que envía no están firmados por DKIM, haga lo siguiente:

- Asegúrese de que DKIM está habilitado para la identidad correcta. Para habilitar DKIM para una identidad en la consola de Amazon SES, elija el dominio de correo electrónico en la lista Identities (Identidades). En la página de detalles del dominio, expanda DKIM y, a continuación, seleccione Enable (Habilitar) para habilitar DKIM.
- Asegúrese de que no realiza el envío desde una dirección de correo electrónico verificada en el mismo dominio. Si configura DKIM para un dominio, todos los mensajes que envíe desde ese dominio estarán firmados por DKIM, excepto las direcciones de correo electrónico que haya verificado individualmente. Las direcciones de correo electrónico verificadas individualmente utilizan ajustes independientes. Por ejemplo, si ha configurado DKIM para el dominio example.com y ha verificado por separado la dirección de correo electrónico mary@example.com (pero no ha configurado DKIM para la dirección), los mensajes de correo electrónico que envíe desde mary@example.com se enviarán sin autenticación de DKIM. Puede resolver este problema si elimina la identidad de la dirección de correo electrónico de la lista de identidades de su cuenta.
- Si utiliza la misma identidad en más de una región de AWS, deberá configurar DKIM para cada región por separado. Del mismo modo, si utiliza el mismo dominio con más de una cuenta de AWS, deberá configurar DKIM para cada cuenta. Si elimina los registros DNS necesarios para

una región o cuenta específica, Amazon SES desactiva el inicio de sesión de DKIM solo para esa región o cuenta. Si se desactiva el inicio de sesión de DKIM, Amazon SES le envía una notificación por correo electrónico.

Los detalles de DKIM del dominio en la consola de Amazon SES muestran DKIM: waiting on sender verification... (DKIM: esperando la verificación del remitente...). DKIM Verification Status: pending verification (estado de verificación de DKIM: verificación pendiente).

Si completa los procedimientos de Easy DKIM o BYODKIM: utilice su propio DKIM para configurar DKIM para un dominio, pero la consola de Amazon SES sigue indicando que la verificación de DKIM está pendiente, haga lo siguiente:

- Espere hasta 72 horas. En casos excepcionales, los registros DNS demoran en estar visibles para Amazon SES.
- Confirme que el registro CNAME (para Easy DKIM) o el registro TXT (para BYODKIM) utilizan el nombre correcto. Algunos proveedores de DNS añaden automáticamente el nombre de dominio a los registros que crea. Por ejemplo, si crea un registro con un nombre de `example._domainkey.example.com`, su proveedor de DNS podría añadir el nombre de su dominio al final de esta cadena, lo que daría como resultado `example._domainkey.example.com.example.com`. Para obtener más información, consulte la documentación de su proveedor de DNS.

Recibe un correo electrónico de Amazon SES que le informa de que su configuración de DKIM ha sido (o será) revocada.

Esto significa que Amazon SES ya no puede encontrar los registros CNAME necesarios (si ha utilizado Easy DKIM) o los registros TXT necesarios (si ha utilizado BYODKIM) en su servidor DNS. El correo electrónico de notificación le informará de la duración en la que debe volver a publicar los registros DNS antes de que se revoque el estado de configuración de DKIM y se deshabilite la firma DKIM. Si su configuración de DKIM se revoca, debe reiniciar el procedimiento de configuración de DKIM desde el principio.

Cuando se intenta configurar BYODKIM, no se realiza el proceso de verificación de DKIM

Asegúrese de que su clave privada utiliza el formato correcto. La clave privada debe estar en formato PKCS #1 o PKCS #8 y utilizar el cifrado RSA de 1024 o 2048 bits. Además, la clave privada debe estar codificada en base64.

Durante la configuración de BYODKIM, recibe un error **`BadRequestException`** cuando intenta especificar una clave pública para el dominio.

Si recibe un error `BadRequestException`, haga lo siguiente:

- Asegúrese de que el selector que especifique para la clave pública contenga entre 1 y 63 caracteres alfanuméricos. El selector no puede incluir puntos u otros símbolos o signos de puntuación.
- Asegúrese de que ha eliminado las líneas de encabezado y pie de página de la clave pública, y que ha eliminado todos los saltos de línea de la clave pública.

Al utilizar Easy DKIM, los servidores DNS devuelven correctamente los registros CNAME de DKIM de Amazon SES, pero devuelven **`SERVFAIL`** para el registro TXT de verificación del dominio.

Es posible que el proveedor de DNS no pueda redirigir los registros CNAME. Amazon SES y los ISP consultan registros TXT. Para cumplir con la especificación de DKIM, sus servidores DNS deben ser capaces de responder a las consultas de registros TXT, así como a consultas de registros CNAME. Si el proveedor DNS no puede responder a las consultas de registros TXT, una alternativa es utilizar Route 53 como proveedor de alojamiento DNS.

Sus correos electrónicos contienen dos firmas de DKIM

La firma de DKIM adicional, que contiene `d=amazonses.com`, se agrega automáticamente mediante Amazon SES. Puede omitirla.

Problemas de entrega de Amazon SES

Después de realizar una solicitud correcta a Amazon SES, el mensaje suele enviarse de inmediato. En otras ocasiones, podría haber un breve retraso. En cualquier caso, puede tener la certeza de que su correo electrónico se enviará.

Cuando Amazon SES envía su mensaje, sin embargo, diversos factores pueden impedir que se envíe correctamente y, en algunos casos, solo sabrá que ha fallado la entrega al no llegar el mensaje enviado. Utilice el siguiente proceso para resolver esta situación.

Si un correo electrónico no llega, pruebe lo siguiente:

- Verifique que ha realizado una solicitud `SendEmail` o `SendRawEmail` para el correo electrónico en cuestión y que ha recibido una respuesta correcta. Si realiza estas solicitudes mediante programación, compruebe los registros de software para asegurarse de que el programa ha realizado la solicitud y ha recibido una respuesta correcta.
- Lea el artículo del blog Three places where your email could get delayed when sending through SES, ya que el problema podría ser en realidad un retraso en lugar de una falta de entrega.

- Compruebe la dirección de correo electrónico del remitente (la dirección del remitente "From") para comprobar que es válida. Compruebe también la dirección Return-Path, que es donde se envían los mensajes de rebote. Si su correo electrónico tiene rebotes, allí encontrará un mensaje de error explicativo.
- Consulte AWS Service Health Dashboard para confirmar que no hay ningún problema conocido con Amazon SES.
- Póngase en contacto con el destinatario del correo electrónico o el ISP del destinatario. Compruebe que el destinatario está utilizando la dirección de correo electrónico correcta y pregunte si ha habido problemas de entrega conocidos con el ISP del destinatario. Además, determine si el correo electrónico llegó pero se filtró como spam.
- Si se ha registrado en un Plan de AWS Support de pago, puede abrir un nuevo caso de soporte técnico. En su correspondencia con nosotros, le rogamos que nos envíe las direcciones de destinatario pertinentes, junto con cualquier ID de solicitud o ID de mensaje devueltos de las respuestas `SendEmail` o `SendRawEmail`.
- Espere a ver si el problema es en realidad un retraso, no un error de entrega permanente. Para combatir los spammers, algunos proveedores de servicios de Internet rechazan temporalmente los mensajes entrantes de servidores de correo electrónico de envío desconocidos. Este proceso, denominado inclusión en lista gris, puede provocar un retraso en la entrega. Amazon SES volverá a intentar enviar estos mensajes. Si la inclusión en la lista gris es el problema, el ISP podría aceptar el correo electrónico en uno de estos reintentos.
- Incluso cuando tenga en cuenta el mayor interés para sus clientes, es posible que encuentre situaciones que afecten a la capacidad de entrega de sus mensajes. Consulte the section called “Consejos y prácticas recomendadas” que le ayudará a garantizar que sus comunicaciones por correo electrónico lleguen a los destinatarios previstos.

Problemas con correos electrónicos recibidos de Amazon SES

En esta sección se describen algunos problemas comunes que puede encontrar cuando recibe mensajes de correo electrónico enviados desde Amazon SES.

El cliente de correo electrónico muestra «enviado a través de amazonses.com» como el origen del correo electrónico

> Algunos clientes de correo electrónico muestran el dominio «via» cuando el dominio del remitente no coincide con el dominio desde el que se envió el correo electrónico (en este caso, amazonses.com). Para obtener más información, consulte Información adicional junto al nombre

del remitente en el sitio web de Support de Gmail. De forma alternativa, puede configurar Correo identificado con claves de dominio (DKIM). Cuando autentica sus correos electrónicos con DKIM, los clientes de correo electrónico no suelen mostrar el dominio "via" porque la firma DKIM muestra que el correo electrónico procede del dominio declarado. Para obtener información acerca de la configuración de DKIM, consulte Autenticación de correo electrónico con DKIM en Amazon SES.

> **Note**
>
> Si ha recibido spam u otros mensajes de correo electrónico no solicitados de un usuario de SES, utilice las herramientas de denuncia de spam de su cliente de correo electrónico y siga los pasos para denunciar el uso indebido del correo electrónico de SES que se indican en Contactar con nosotros.

El mensaje contiene caracteres confusos o sin sentido

Si el mensaje incluye caracteres que no están en el conjunto de caracteres ASCII (como caracteres latinos acentuados, caracteres chinos o caracteres árabes), debe codificar esos caracteres mediante la codificación de caracteres HTML. Puede utilizar herramientas basadas en la web para codificar los caracteres de su correo electrónico, como el Conversor de caracteres HTML en el sitio web de Email On Acid.

De forma alternativa, puede crear el mensaje MIME usted mismo. En el mensaje MIME, puede especificar que el mensaje debe usar la codificación UTF-8. Cuando utiliza la codificación UTF-8, puede usar caracteres que no sean ASCII directamente en sus mensajes. Cuando haya terminado de crear el mensaje MIME, puede enviarlo usando la API SendRawEmail o la API SendMail v2.

Una causa común de este problema es la característica de comillas inteligentes de Microsoft Word. Si a menudo copia contenido de Word y lo pega en sus correos electrónicos, es posible que encuentre este problema. La característica de comillas inteligentes sustituye los caracteres de comillas rectas ("...") por comillas inglesas (“...”). Los caracteres de comillas inglesas no son caracteres ASCII estándar. Como consecuencia, podrían mostrarse en algunos clientes de correo electrónico como “??” o como un grupo de caracteres como “â€œ”. Para resolver este problema, puede deshabilitar la característica de citas inteligentes en Word. De forma alternativa, puede utilizar la solución SendRawEmail del párrafo anterior. Para obtener información sobre cómo

deshabilitar esta característica, consulte Comillas inteligentes en Word en el sitio web de Support de Microsoft Office.

Problemas de notificaciones de Amazon SES

Si tiene un problema con las notificaciones de rebotes, reclamaciones o notificaciones, revise las posibles causas y soluciones que aparecen a continuación.

- Recibe notificaciones de rebote a través de Amazon SNS , pero no sabe a qué destinatarios corresponden las notificaciones: en el futuro, para asociar una notificación de rebote con un determinado destinatario, dispone de las siguientes opciones:
  - Habida cuenta de que Amazon SES no mantiene los ID de mensaje personalizados que se agregan, almacene un mapeo entre un identificador y el ID de mensaje de Amazon SES que le devuelve Amazon SES cuando acepta el correo electrónico.
  - En cada llamada a Amazon SES, realice en envío a un único destinatario, en lugar de enviar un único mensaje a varios destinatarios.
  - Puede habilitar el reenvío de retroalimentación por correo electrónico, que le reenviará el mensaje de rebote completo.
- Puede recibir quejas o entregar notificaciones a través de Amazon SNS o del reenvío de retroalimentación de correo electrónico, pero no sabe a qué destinatarios corresponden las notificaciones: algunos ISP redactan la dirección de correo electrónico del destinatario que ha reclamado antes de transferir la notificación de reclamo a Amazon SES. Para permitirle encontrar la dirección de correo electrónico del destinatario, la mejor opción consiste en almacenar su propio mapeo entre un identificador y el ID de mensaje de Amazon SES que le devuelve Amazon SES cuando acepta el correo electrónico. Tenga en cuenta que Amazon SES no mantiene ningún ID de mensaje personalizado que agrega.
- Desea configurar notificaciones para ir a un tema de Amazon SNS que no es de su propiedad: el propietario de dicho tema debe configurar una política de acceso de Amazon SNS que permita a su cuenta llamar a la acción `SNS:Publish` en su tema. Para obtener información acerca de cómo controlar el acceso a su tema de Amazon SNS a través del uso de políticas de IAM, consulte Administración del acceso a los temas de Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.

Errores de envío de correo electrónico de Amazon SES

En este tema se revisan tipos de errores específicos de envío de correo electrónico que podría encontrar al enviar un correo electrónico a través de Amazon SES. Si intenta enviar un correo electrónico a través de Amazon SES y la llamada a Amazon SES falla, Amazon SES devuelve un mensaje de error a la aplicación y no envía el correo electrónico. La forma en que observa este mensaje de error depende de la forma en que llama a Amazon SES.

- Si llama a la API de Amazon SES directamente, la acción de consulta devolverá un error. El error puede ser `MessageRejected` o uno de los errores que se especifican en el tema Errores comunes de la Referencia de la API de Amazon Simple Email Service.
- Si llama a Amazon SES utilizando un SDK de AWS que utilice un lenguaje de programación que admita excepciones, Amazon SES podría lanzar una excepción. El tipo de excepción depende del SDK y del error. Por ejemplo, podría tratarse de una excepción `MessageRejectedException` de Amazon SES (el nombre real puede variar en función del SDK) o una excepción general de AWS. Independientemente del tipo de excepción, el tipo de error y el mensaje de error de la excepción podrían darle más información.
- Si llama a Amazon SES a través de su interfaz de SMTP, la forma en que experimenta el error depende de la aplicación. Es posible que algunas aplicaciones muestren un mensaje de error específico y que otras no. Para obtener una lista de los códigos de respuesta SMTP que devuelve Amazon SES, consulte Códigos de respuesta de SMTP devueltos por Amazon SES..

> **Note**
>
> Si su llamada a Amazon SES para enviar un correo electrónico devuelve un error, no se le facturará dicho correo electrónico.

A continuación se indican los tipos de problemas específicos de Amazon SES que pueden hacer que Amazon SES devuelva un error cuando se intenta enviar un correo electrónico. Estos errores se agregan a errores de AWS generales como `MalformedQueryString`, tal y como se especifica en el tema Errores comunes de la Referencia de la API de Amazon Simple Email Service.

- La dirección de correo electrónico no está verificada. Las siguientes identidades no han superado la verificación en la región region: identity1, identity2, identity3: está intentando enviar correo electrónico desde una dirección de correo electrónico o un dominio que no ha verificado con

Amazon SES. Este error podría corresponder a la dirección "From", "Source", "Sencer" o "Return-Path". Si su cuenta sigue todavía en el entorno de pruebas de Amazon SES, también debe verificar todas las direcciones de correo electrónico de cada destinatario excepto los destinatarios que proporciona el simulador de buzón de correo de Amazon SES. Si Amazon SES no puede mostrar todas las identidades con errores, el mensaje de error termina con puntos suspensivos.

> **Note**
>
> Amazon SES tiene puntos de enlace en varias Regiones de AWS y el estado de verificación de cada dirección de correo electrónico es independiente para cada Región de AWS. Debe completar el proceso de verificación para cada remitente de las Regiones de AWS que desee utilizar.

- La cuenta está suspendida: se ha suspendido la capacidad de su cuenta para enviar correo electrónico. Puede seguir accediendo a la consola de Amazon SES y realizar la mayoría de las operaciones. Sin embargo, si intenta enviar un correo electrónico, recibe este mensaje.

  Si suspendemos la capacidad de su cuenta para enviar correo electrónico, enviamos automáticamente una notificación a la dirección de correo electrónico asociada con su Cuenta de AWS. Para obtener más información, consulte the section called “Preguntas frecuentes sobre el proceso de revisión de envío”.

- Limitación controlada: es posible que su aplicación esté intentando enviar demasiados mensajes por segundo o que haya enviado demasiados correos electrónicos durante las últimas 24 horas. En estos casos, el mensaje de error puede ser similar a los siguientes ejemplos:

  - Cuota de mensajes diaria superada: ha enviado el número máximo de mensajes permitidos en un periodo de 24 horas. Si ha superado su cuota diaria, tendrá que esperar hasta el próximo periodo de 24 horas antes de poder enviar más mensajes.
  - Velocidad máxima de envío superada: está intentando enviar más correos electrónicos por segundo de lo que permite la velocidad máxima de envío. Si ha superado la tasa de envío, puede seguir enviando correo electrónico, pero tendrá que reducir la tasa de envío. Para obtener más información, consulte How to handle a “Throttling - Maximum sending rate exceeded” error en el Blog de mensajería y segmentación de AWS.
  - Se ha superado la velocidad máxima de envío de SMTP SigV2: está intentando enviar mensajes con credenciales SMTP creadas antes del 10 de enero de 2019; sus credenciales SMTP se crearon utilizando una versión anterior de AWS Signature. Por motivos de seguridad, debe eliminar las credenciales que creó antes de esa fecha y reemplazarlas por otras nuevas. Puede

eliminar las credenciales antiguas mediante la consola de IAM. Para obtener más información acerca de cómo crear credenciales, consulte the section called “Obtención de las credenciales de SMTP”.

Debería monitorizar periódicamente su actividad de envío para ver lo cerca que está de sus cuotas de envío. Para obtener más información, consulte Monitoreo de las cuotas de envío de Amazon SES. Para obtener información general sobre las cuotas de envío, consulte Administración de sus límites de envío de Amazon SES. Para obtener información sobre cómo aumentar sus cuotas de envío, consulte Aumento de las cuotas de envío de Amazon SES.

> **Important**
>
> Si el texto de error que explica el error de limitación controlada no está relacionado con que supere la cuota diaria o la tasa de envío máxima, entonces podría haber un problema en todo el sistema que está provocando una reducción de las capacidades de envío. Para obtener información acerca del estado del servicio, vaya a AWS Service Health Dashboard.

- No se han especificado destinatarios: no se han proporcionado destinatarios.
- Hay caracteres no ASCII en la dirección de correo electrónico: la cadena de la dirección de correo electrónico debe ser ASCII de 7 bits. Si desea enviar a direcciones de correo electrónico que contengan caracteres Unicode en la parte de dominio de una dirección o bien desde ellas, debe cifrar el dominio utilizando Punycode. Punycode no se permite en la parte local de la dirección de correo electrónico (la parte delante del signo @) ni en el nombre de "remitente descriptivo". Si desea utilizar caracteres Unicode en el nombre de "remitente descriptivo", debe codificar el nombre de "remitente descriptivo" utilizando la sintaxis de palabra cifrada MIME, tal y como se describe en Envío de correo electrónico sin procesar mediante la API v2 de Amazon SES. Para obtener más información acerca de Punycode, consulte RFC 3492.
- El dominio MAIL FROM no se ha verificado: Amazon SES no ha podido leer el registro MX necesario para utilizar el dominio MAIL FROM especificado. Para obtener información sobre la configuración de dominios MAIL FROM personalizados, consulte Uso de un dominio MAIL FROM personalizado.
- El conjunto de configuración no existe: el conjunto de configuración que ha especificado no existe. Un conjunto de configuración es un parámetro opcional que utiliza para publicar eventos de envío de correo electrónico. Para obtener más información, consulte Monitoreo del envío de correo electrónico mediante la publicación de eventos de Amazon SES.

Aumento del rendimiento con Amazon SES

Al enviar correos electrónicos, puede llamar a Amazon SES con la frecuencia que permita su velocidad máxima de envío. (Para obtener más información sobre el ratio máximo de envío, consulte Administración de sus límites de envío de Amazon SES). Sin embargo, cada llamada a Amazon SES tarda tiempo en completarse.

Si realiza varias llamadas a Amazon SES utilizando la API de Amazon SES o la interfaz de SMTP, es posible que desee poner en práctica los siguientes consejos para mejorar el rendimiento:

- Mida el rendimiento actual para identificar cuellos de botella: una posible prueba de rendimiento implica el envío de varios correos electrónicos de prueba lo más rápidamente posible dentro de un bucle de código en su aplicación. Mida la latencia de ida y vuelta de cada solicitud `SendEmail`. A continuación, lance gradualmente instancias adicionales de la aplicación en la misma máquina y analice el impacto en la latencia de red. Es posible que también desee ejecutar esta prueba en varias máquinas y en distintas redes para ayudar a identificar los posibles cuellos de botella en los recursos de las máquinas o los cuellos de botella de red que puedan existir.
- (Solo API) Plantéese utilizar conexiones HTTP persistentes: en lugar de incurrir en los costos que supone establecer una nueva conexión HTTP independiente para cada solicitud de la API, utilice las conexiones HTTP persistentes. Es decir, vuelva a utilizar la misma conexión HTTP para varias solicitudes de la API.
- Considere la posibilidad de utilizar varios subprocesos: cuando una aplicación utiliza un único hilo, el código de la aplicación llama a la API de Amazon SES y, a continuación, espera de forma sincrónica una respuesta de la API. El envío de correos electrónicos suele ser una operación vinculada a E/S y realizar el trabajo desde varios subprocesos ofrece un mejor rendimiento. Puede enviar de forma simultánea utilizando tantos subprocesos de ejecución como desee.
- Considere la posibilidad de utilizar varios procesos: el uso de varios procesos puede contribuir a aumentar el rendimiento, ya que tendrá más conexiones activas simultáneas para Amazon SES. Por ejemplo, puede segmentar sus correos electrónicos previstos en varios buckets y, a continuación, ejecutar varias instancias de su script de envío de correo electrónico simultáneamente.
- Plantéese la posibilidad de utilizar un relé de correo local: su aplicación puede transmitir mensajes rápidamente a su servidor de correo local, lo que puede contribuir a almacenar los mensajes en el búfer y a transmitirlos de forma asíncrona a Amazon SES. Algunos servidores de correo admiten la simultaneidad de entrega, lo que significa que, aunque la aplicación esté generando correos electrónicos para el servidor de correo en un solo subproceso, el servidor de correo utilizará varios

subprocesos al enviarlos a Amazon SES. Para obtener más información, consulte Integración de Amazon SES con su servidor de correo electrónico existente.

- Plantéese alojar su aplicación más cerca del punto de enlace de la API de Amazon SES: es posible que desee plantearse el alojamiento en un centro de datos próximo al punto de enlace de la API de Amazon SES o una instancia de Amazon EC2 en la misma región de AWS que el punto de enlace de la API de Amazon SES. Esto puede ayudar a reducir la latencia de red entre su aplicación y Amazon SES y mejorar el rendimiento. Para ver una lista de las regiones donde Amazon SES está disponible, consulte Amazon Simple Email Service (Amazon SES) en la Referencia general de AWS.
- Plantéese la posibilidad de utilizar varias máquinas: en función de la configuración en su equipo anfitrión, es posible que haya un límite en el número de conexiones HTTP simultáneas a una única dirección IP, que podría limitar los beneficios del paralelismo, una vez se supera un determinado número de conexiones simultáneas en una única máquina. Si se trata de un cuello de botella, es posible que desee realizar solicitudes de Amazon SES simultáneas utilizando varias máquinas.
- Plantéese la posibilidad de utilizar la API de consulta de Amazon SES en lugar del punto de enlace de SMTP: el uso de la API de consulta de Amazon SES le permite enviar la solicitud de envío de correo electrónico a través de una única llamada de red, mientras que interactuar con el punto de enlace de SMTP implica una conversación de SMTP que consta de varias solicitudes de red (por ejemplo, EHLO, MAIL FROM, RCPT TO, DATA, QUIT). Para obtener más información acerca de la API de consulta de Amazon SES, consulte Uso de la API de Amazon SES para enviar correo electrónico.
- Utilice el simulador de buzón de correo de Amazon SES para probar su rendimiento máximo: para probar cualquier cambio que pueda implementar, puede utilizar el simulador de buzón de correo. El simulador de bandeja de correo puede ayudarle a determinar el rendimiento máximo del sistema sin gastar su cuota de envío diaria. Para obtener información sobre el simulador de bandeja de correo, consulte Uso del simulador de buzón de correo de forma manual.

Si va a acceder a Amazon SES a través de su interfaz de SMTP, consulte Problemas de SMTP de Amazon SES para ver problemas específicos relacionados con SMTP que puedan afectar al rendimiento.

Problemas de SMTP de Amazon SES

Esta sección contiene soluciones para varios problemas comunes relacionados con el envío de correo electrónico a través de la interfaz Simple Mail Transfer Protocol (SMTP) de Amazon SES. También contiene una lista de códigos de respuesta SMTP que devuelve Amazon SES.

Para obtener más información acerca del envío de correo electrónico a través de la interfaz SMTP de Amazon SES, consulte Uso de la interfaz de SMTP de Amazon SES para enviar correo electrónico.

- No se puede conectar al punto de enlace SMTP de Amazon SES.

  Los problemas para conectarse al punto de enlace de SMTP de Amazon SES suelen estar relacionados con los siguientes problemas:

  - Credenciales incorrectas: las credenciales que usa para conectarse al punto final SMTP son diferentes de AWS las suyas. Para conseguir sus credenciales de SMTP, consulte Obtención de las credenciales de SMTP de Amazon SES. Para obtener más información acerca de las credenciales, consulte Tipos de credenciales de Amazon SES.
  - Problemas de red o del firewall: es posible que su red esté bloqueando las conexiones salientes a través del puerto desde el que está intentando enviar correo electrónico. Para determinar si un problema en la red local está causando problemas de conexión, escriba el siguiente comando en la línea de comandos, sustituyendo *`port`* por el puerto que intenta utilizar (normalmente, 465, 587, 2465 o 2587): `telnet email-smtp.us-west-2.amazonaws.com` *`port`*

    Si puede conectarse al servidor SMTP a través de este comando, e intenta conectarse a Amazon SES mediante TLS Wrapper o STARTTLS, realice los procedimientos que se muestran en Prueba de la conexión a la interfaz SMTP de Amazon SES mediante la línea de comandos.

    Si no puede conectarse al punto de enlace de SMTP de Amazon SES con `telnet` u `openssl`, significa que hay algo en su red (por ejemplo, un firewall) que bloquea las conexiones salientes a través del puerto que está intentando utilizar. Trabaje con el administrador de red para diagnosticar y corregir el problema.
- Está enviando correo electrónico a Amazon SES desde una instancia de Amazon EC2 usando el puerto 25 y recibe mensajes de tiempo de espera agotado.

  Amazon EC2 restringe el puerto 25 de forma predeterminada. Para eliminar estas restricciones, envíe una solicitud de Amazon EC2 para eliminar las limitaciones de envío de correo electrónico. También puede conectarse a Amazon SES a través de los puertos 465 o 587, ya que ninguno de estos puertos está restringido.
- Se borran los mensajes de correo electrónico debido a errores de red.

  Asegúrese de que su aplicación utiliza la lógica de reintentos cuando se conecta al punto de enlace de SMTP de Amazon SES y de que puede detectar y reintentar la entrega de mensajes en caso de un error de red. SMTP es un protocolo detallado y el envío de un correo electrónico a

través de este protocolo requiere varios viajes de red de ida y vuelta. Debido a la naturaleza de SMTP, el potencial de los errores de red aumenta.

- Ha perdido la conexión con el punto de enlace de SMTP.

  Las conexiones perdidas se deben generalmente a los siguientes problemas:

  - Tamaño de MTU: si recibe un mensaje de error de tiempo de espera superado, el tamaño de la unidad de transmisión máxima (MTU) de la interfaz de red de la computadora que utilice para conectarse SMTP de Amazon SES podría ser demasiado grande. Para solucionar este problema, establezca el tamaño de MTU en ese equipo en 1 500 bytes.

    Para obtener más información acerca de cómo definir el tamaño de MTU en los sistemas operativos Windows, Linux y macOS, consulte Falta de respuesta de las consultas y pérdidas de consultas antes de llegar al clúster en la Guía de administración de Amazon Redshift.

    Para obtener más información sobre cómo configurar el tamaño de MTU para una instancia de Amazon EC2, consulte la Unidad máxima de transmisión de red (MTU) para la instancia de EC2 en la Guía del usuario de Amazon EC2.

  - Conexiones de larga duración: el punto de enlace SMTP de Amazon SES se ejecuta en una flota de instancias de Amazon EC2 detrás de una instancia de Elastic Load Balancer (ELB). Para garantizar que el sistema sea tolerante a errores, up-to-date las instancias Amazon EC2 activas se cancelan periódicamente y se sustituyen por nuevas instancias. Dado que su aplicación se conecta a una instancia de Amazon EC2 a través del ELB, la conexión deja de ser válida cuando la instancia de Amazon EC2 se termina. Debe establecer una nueva conexión SMTP después de haber entregado un número fijo de mensajes por medio de una única conexión SMTP o si la conexión SMTP ha estado activa durante cierto periodo de tiempo. Tendrá que experimentar para buscar umbrales adecuados en función de dónde se aloja la aplicación y cómo envía correo electrónico a Amazon SES.

- Le convendrá conocer las direcciones IP de los servidores de correo SMTP de Amazon SES para poder incluir en la lista de permitidos dichas direcciones IP con la red.

  Las direcciones IP de los puntos de enlace de SMTP de Amazon SES se encuentran detrás de balanceadores de carga. Como resultado, estas direcciones IP cambian con frecuencia. No es posible proporcionar una lista definitiva de todas las direcciones IP de los puntos de enlace de Amazon SES. Le recomendamos que incluya en la lista de permitidos el dominio `amazonses.com`, en lugar de incluir en la lista de permitidos direcciones IP individuales.

Códigos de respuesta de SMTP devueltos por Amazon SES.

Esta sección contiene una lista de códigos de respuesta que devuelve la interfaz SMTP de Amazon SES.

Debe volver a intentar las solicitudes SMTP que reciban errores 400. Le recomendamos que implemente un sistema que vuelva a intentar las solicitudes con tiempos de espera progresivamente más largos (por ejemplo, esperar 5 segundos antes de volver a intentar; a continuación, esperar 10 segundos y, seguidamente, esperar 30 segundos). Si el tercer reintento no se realiza correctamente, espere 20 minutos y, a continuación, repita el proceso. Para ver un ejemplo de una implementación que utilice una política de reintentos exponencial, consulte How to handle a "Throttling - Maximum sending rate exceeded" error en el Blog de mensajería y segmentación de AWS .

> **Note**
>
> AWS Los SDK implementan la lógica de reintento automáticamente, pero utilizan la interfaz HTTPS en lugar de SMTP.

Si recibe un error 500, tiene que revisar su solicitud para corregir un problema antes de volver a enviar la solicitud. Por ejemplo, si sus credenciales de AWS autenticación no son válidas, debe actualizar la aplicación para que utilice las credenciales correctas antes de volver a enviar la solicitud.

Descripción	Código de respuesta	Más información
Autenticación correcta	`235 Authentication successful`	El cliente de SMTP se conecta correctamente e inicia sesión en el servidor SMTP.
Entrega satisfactoria	`250 Ok` *`MessageID`*	*`MessageID`* es una cadena de caracteres única que Amazon SES utiliza para identificar un mensaje.
Servicio no disponible	`421 Too many concurrent SMTP connections`	Amazon SES no puede procesar la solicitud ya que actualmente

Descripción	Código de respuesta	Más información
		hay demasiadas conexiones al servidor SMTP.
Error de procesamiento local	`451 Temporary service failure`	Amazon SES no ha podido procesar la solicitud. Es posible que haya problemas con la solicitud de carga que le impidan su procesamiento.
Tiempo de espera	`451 Timeout waiting for data from client`	Ha transcurrido demasiado tiempo entre las solicitudes, por lo que el servidor SMTP cerró la conexión.
Cuota de envío diaria superada	`454 Throttling failure: Daily message quota exceeded`	Ha superado el número máximo de mensajes de correo electrónico que le permite enviar Amazon SES en un periodo de 24 horas. Para obtener más información, consulte Administración de sus límites de envío de Amazon SES.
Tasa de envío máxima superada	`454 Throttling failure: Maximum sending rate exceeded`	Ha superado el número máximo de mensajes de correo electrónico que le permite enviar Amazon SES por segundo. Para obtener más información, consulte Administración de sus límites de envío de Amazon SES.

Descripción	Código de respuesta	Más información
Problema de Amazon SES al validar las credenciales de SMTP	`454 Temporary authentication failure`	Entre los problemas que podría provocar esto se incluyen (entre otros): • Hay un problema con el cifrado entre su aplicación de envío de correo electrónico y Amazon SES. Tenga en cuenta que tiene que utilizar una conexión cifrada al conectarse a Amazon SES. Para obtener más información, consulte Conexión a un punto de enlace de SMTP de Amazon SES. • Amazon SES podría experimentar un problema. Consulte AWS Service Health Dashboard para buscar actualizaciones.
Problema al recibir la solicitud	`454 Temporary service failure`	Amazon SES no ha recibido correctamente la solicitud. Como resultado, el mensaje no se ha enviado.
Credenciales incorrectas	`530 Authentication required`	La aplicación que utiliza para enviar correo electrónico no intentó autenticarse cuando se conectó a la interfaz SMTP de Amazon SES.

Descripción	Código de respuesta	Más información
Credenciales de autenticación no válidas	`535 Authentication Credentials Invalid`	La aplicación que utiliza para enviar correo electrónico no facilitó las credenciales de SMTP correctas a Amazon SES. Tenga en cuenta que sus credenciales SMTP no son las mismas que sus AWS credenciales. Para obtener más información, consulte Obtención de las credenciales de SMTP de Amazon SES.
Cuenta no suscrita a Amazon SES	`535 Account not subscribed to SES`	El Cuenta de AWS propietario de las credenciales SMTP no está registrado en Amazon SES.
El mensaje es demasiado largo	`552 Message is too long.`	El mensaje que intenta enviar es más grande que el tamaño de mensaje máximo.
Cuenta no suscrita a Amazon SES	`535 Account not subscribed to SES`	El Cuenta de AWS propietario de las credenciales SMTP no está registrado en Amazon SES.
Error de sintaxis MAIL FROM	`553 <email-address > Invalid email address`	Hay un error de sintaxis en la parte MAIL FROM del mensaje de SMTP. Compruebe que sigue el formato correcto y no olvide incluir la dirección de correo electrónico en "**<>**".

Descripción	Código de respuesta	Más información
Error de sintaxis RCPT TO	`553 <email-address > address unknown`	Hay un error de sintaxis en la parte RCPT TO del mensaje de SMTP. Compruebe que sigue el formato correcto y no olvide incluir la dirección de correo electrónico en "**<>**".
Usuario no autorizado a llamar al punto de enlace de SMTP de Amazon SES	`554 Access denied: User UserARN is not authorized to perform ses:SendRawEmail on resource IdentityARN`	La política AWS Identity and Access Management (IAM) o la política de autorización de envío de Amazon SES del usuario propietario de las credenciales SMTP no pueden llamar al punto de conexión SMTP de Amazon SES.

Descripción	Código de respuesta	Más información
Dirección de correo electrónico sin verificar	`554 Message rejected: Email address is not verified. The following identities failed the check in region region: identity0 , identity1 , identity2`	Está intentando enviar correo electrónico desde una dirección de correo electrónico o dominio que no está verificado para enviar correo electrónico desde su cuenta de Amazon SES. Este error podría corresponder a las direcciones "From", "Source", "Sencer" o "Return-Path". Si su cuenta sigue todavía en el entorno de pruebas, también tiene que verificar todas las direcciones de correo electróni co de cada destinatario (excepto de aquellos que proporciona el simulador de buzón de correo de Amazon SES). Si Amazon SES no puede mostrar todas las identidades que no han superado la comprobación de verificación, el mensaje de error termina con tres puntos (...). **Note** Amazon SES tiene puntos de enlace en varios Regiones de AWS y el estado de verificación de la dirección de correo electrónico es independi ente para cada uno Región de AWS. Debe completar el proceso de

Descripción	Código de respuesta	Más información
		verificación para cada remitente Regiones de AWS que desee utilizar.

> **Note**
>
> En el caso de problemas de SMTP que no se solucionen con la resolución de problemas de esta página, pruebe las opciones de asistencia de SES que aparecen en la sección Contactar con nosotros.

Preguntas frecuentes sobre Amazon SES

Esta sección contiene respuestas a varias preguntas frecuentes relacionadas con el uso de Amazon SES.

Esta sección contiene preguntas frecuentes sobre los siguientes temas:

- Preguntas frecuentes acerca del proceso de revisión de envío de Amazon SES
- Preguntas frecuentes acerca de la lista de agujeros negros de DNS (DNSBL)
- Preguntas frecuentes sobre métricas de envío de correo electrónico de Amazon SES

Preguntas frecuentes acerca del proceso de revisión de envío de Amazon SES

Monitoreamos el correo electrónico que se envía a través de Amazon SES para asegurarnos de que el servicio no se está utilizado para enviar correo electrónico malintencionado, no solicitado o de baja calidad. Si determinamos que un usuario está enviando contenido que entra dentro de una de estas categorías, tomamos medidas en esa cuenta. Este proceso lo denominamos proceso de revisión de envío.

En muchos casos, cuando detectamos un problema con una cuenta, ponemos dicha cuenta en proceso de revisión. En otros casos, suspendemos la capacidad de la cuenta para enviar correo electrónico. Tomamos estas medidas para proteger la reputación de remitente de cada cuenta y para evitar que otros usuarios de SES sufran interrupciones del servicio y problemas de entrega.

Contenido

- Preguntas frecuentes sobre cuentas en proceso de revisión
- Preguntas frecuentes sobre la suspensión del envío
- Preguntas frecuentes sobre rebotes
- Preguntas frecuentes sobre reclamaciones
- Preguntas frecuentes sobre trampas de spam
- Preguntas frecuentes sobre investigaciones manuales

Preguntas frecuentes sobre cuentas en proceso de revisión

Q1 (P1). He recibido un mensaje que indica que mi cuenta está en proceso de revisión. ¿Eso qué significa?

Hemos detectado un problema relacionado con el correo electrónico enviado desde su cuenta y le estamos dando tiempo para solucionarlo. Puede seguir enviando correo electrónico como lo haría normalmente, pero también debe corregir el problema que ha hecho que la cuenta esté en proceso de revisión. Si no corrige el problema antes de que finalice el periodo de revisión, podríamos suspender su capacidad de enviar correo electrónico adicional.

Q2 (P2). ¿Recibiré siempre una notificación si mi cuenta se pone en proceso de revisión?

Sí. Recibirá una notificación en la dirección de correo electrónico asociada a su cuenta de AWS .

Q3 (P3). ¿Por qué he recibido una notificación de que mi cuenta está en proceso de revisión?

Cuando se revisa su cuenta, automáticamente le enviamos una notificación a la dirección de correo electrónico asociada a su AWS cuenta. Esta dirección de correo electrónico es la que especificó al crear su AWS cuenta. En algunos casos, esta dirección de correo electrónico puede ser diferente de la que usó para enviar correos electrónicos a través de SES.

Le recomendamos que monitoree su reputación de remitente con regularidad consultando las métricas de reputación. También puedes configurar alarmas automáticas en Amazon CloudWatch. Estas alarmas pueden enviarle una notificación cuando sus métricas de reputación superen determinados umbrales. También puedes configurar Amazon CloudWatch para que se ponga en contacto contigo de otras formas, por ejemplo, enviando un mensaje de texto a tu teléfono móvil.

P4. ¿El hecho de que mi cuenta de SES esté siendo objeto de revisión afectará a mi uso de otros AWS servicios?

Podrás seguir utilizando otros AWS servicios mientras se esté revisando tu cuenta de SES. Sin embargo, si solicita un aumento de la cuota de servicio para otro AWS servicio que envía comunicaciones salientes (como Amazon SNS), es posible que se deniegue esa solicitud hasta que se suspenda el período de revisión de su cuenta de SES.

P5. ¿Qué debo hacer si mi cuenta se encuentra en proceso de revisión?

Debe hacer lo siguiente:

- Si la situación lo permite, deje de enviar correo hasta que solucione el problema. Puede seguir enviando correo electrónico mientras su cuenta está en proceso de revisión. Sin embargo, si sigue enviando correo sin realizar cambios, es posible que empeore el problema sin darse cuenta.
- Consulte el correo electrónico que le hemos enviado para conocer un resumen del problema.
- Investigue sus envíos para determinar qué aspectos de su envío han desencadenado específicamente el problema.
- Tras realizar los cambios que crea que resolverán el problema, inicie sesión en la AWS consola y vaya al Support Center. Responda al caso que abrimos en su nombre. En su mensaje, proporcione información detallada sobre las medidas que ha tomado para resolver el problema y explique de qué manera estos pasos evitarán que el problema vuelva a producirse en el futuro.
- Asegúrese de facilitar toda la información que le solicitemos específicamente. Necesitamos esta información para evaluar su caso.

P6. ¿Cómo puedo solicitar una revisión?

Puedes solicitar que revisemos nuestra decisión de revisar tu cuenta. Para solicitar una revisión, inicie sesión en la AWS consola y vaya al Support Center. Responda al caso que abrimos en su nombre.

En la solicitud, proporcione la siguiente información:

- Información sobre la causa principal del evento que provocó que la cuenta se sometiera a un proceso de revisión.
- Una lista de los cambios que ha realizado para corregir el problema. Incluya solo los pasos que ya ha implementado, no los que piensa implementar en el futuro.
- Información sobre cómo estos cambios evitan que el mismo problema se repita en el futuro.

Dependiendo de la naturaleza del evento por el que pusimos su cuenta en proceso de revisión, podríamos solicitar información adicional. Consulte el tema de las preguntas frecuentes relacionado con el problema que tuvo para obtener una lista de la información que debe incluir en la solicitud.

P7. ¿Qué ocurre si no se acepta mi solicitud de revisión?

Responderemos a su solicitud con información acerca de por qué no la hemos aceptado. En algunos casos, podrá enviar otra solicitud si puede demostrar que ha resuelto el problema, y que los cambios evitarán que el problema se repita en el futuro.

P8. ¿Puede ayudarme a diagnosticar el problema?

Normalmente podemos facilitarle solo información general de alto nivel sobre su problema (por ejemplo, que tiene un problema de rebotes). Tendrá que investigar por su parte la causa raíz.

P9. ¿Cómo puedo saber si mi cuenta ya no está en proceso de revisión?

Las métricas de reputación incluyen información acerca del estado actual de su cuenta. Para obtener más información, consulte Uso de métricas de reputación para realizar un seguimiento de las tasas de rebotes y de reclamos.

P10. ¿Ponen mi cuenta en proceso de revisión cada vez que hay un problema?

No. En algunas situaciones, podríamos suspender la capacidad de su cuenta para enviar correo electrónico sin ponerla antes en proceso de revisión. Por ejemplo:

- Si el problema es muy grave.
- Si la cuenta se ha puesto en proceso de revisión por el mismo problema varias veces en el pasado. Por este motivo, es importante abordar el problema subyacente en lugar de solucionar únicamente el incidente específico que provocó que la cuenta se pusiera en proceso de revisión. Por ejemplo, si una campaña determinada ha hecho que la cuenta se ponga en proceso de revisión, debe hacer algo más que simplemente a detener dicha campaña. Debe determinar qué propiedades de la campaña resultaron problemáticas y asegurarse de implantar procesos para que sus futuras campañas no tengan el mismo problema.

En cualquiera de estas situaciones, se le enviará una notificación automáticamente cuando se detenga la capacidad de su cuenta para enviar correo electrónico.

P11. ¿Qué ocurre si realizo las correcciones poco antes de que venza mi proceso de revisión?

Inicie sesión AWS Management Console y vaya al Support Center. Responda al caso que abrimos en su nombre. En su respuesta al caso, háganos saber que ha resuelto el problema.

P12. ¿Puedo obtener ayuda de mi AWS representante o de Premium Support?

Si ya estás trabajando con un representante de AWS cuentas, nos pondremos en contacto con él automáticamente cuando se revise tu cuenta. Su representante de cuenta podría facilitarle información adicional para ayudarle a comprender mejor el problema. Si utiliza Premium Support, también debería ponerse en contacto con dicho equipo para obtener más ayuda.

Preguntas frecuentes sobre la suspensión del envío

Q1 (P1). He recibido un mensaje que indica que la capacidad de mi cuenta para enviar correo electrónico se ha suspendido. ¿Eso qué significa?

Hemos suspendido la capacidad de su cuenta para enviar correo electrónico debido a un problema crítico con los mensajes que ha enviado. En la mayoría de los casos, suspendemos las cuentas por alguna de las razones siguientes:

- Ya habíamos puesto antes su cuenta en proceso de revisión. Los problemas que han provocado que su cuenta esté en proceso de revisión no se han corregido antes del final del periodo de revisión, por lo que hemos suspendido la capacidad de su cuenta para enviar correo electrónico.
- Hemos puesto su cuenta en proceso de revisión varias veces para el mismo problema.
- Su cuenta envió correo electrónico que infringía las Condiciones del servicio de AWS. Si estas infracciones son graves, podríamos suspender la capacidad de su cuenta para enviar correo electrónico sin ponerla antes en proceso de revisión.

Q2 (P2). ¿Recibiré siempre una notificación si la capacidad de mi cuenta para enviar correo electrónico se suspende?

Sí. Recibirá una notificación en la dirección de correo electrónico asociada a su cuenta de AWS .

Q3 (P3). Se ha suspendido la capacidad de mi cuenta para enviar correo electrónico. ¿Por qué no recibo una notificación?

Cuando suspendemos la capacidad de una cuenta para enviar correo electrónico, enviamos automáticamente una notificación a la dirección de correo electrónico asociada con esa cuenta.

> **Note**
>
> Al crear su AWS cuenta, debe proporcionar una dirección de correo electrónico. Puede cambiar esta dirección en cualquier momento. Para obtener más información sobre cómo cambiar la dirección asociada a su AWS cuenta, consulte Administrar una AWS cuenta en la Guía del AWS Billing and Cost Management usuario.

Puedes usar Amazon CloudWatch para crear alarmas que te informen cuando tus porcentajes de devoluciones y quejas sean demasiado altos. La creación de una alarma es una buena manera de recibir una advertencia temprana de los factores que podrían hacer que detengamos la capacidad de su cuenta para enviar correo electrónico. Sin embargo, hay factores distintos de los rebotes y las reclamaciones que podrían provocar que detuviéramos su capacidad para enviar correo electrónico. Para obtener más información sobre cómo crear alarmas en CloudWatch, consultaCreación de alarmas de monitoreo de reputación en CloudWatch.

También puede utilizar el panel de cuenta para determinar el estado actual de la cuenta. Por ejemplo, si la capacidad de la cuenta para enviar correo electrónico actualmente está suspendida, la sección Account status (Estado de la cuenta) del panel de la cuenta muestra el estado Paused (Suspendido). Si la cuenta puede enviar correo electrónico con normalidad, muestra el estado Healthy (Correcto).

Por último, puedes consultar el AWS Health Dashboard (PHD) en https://phd.aws.amazon.com/ para determinar si la capacidad de tu cuenta para enviar correos electrónicos está pausada actualmente. Cuando suspendemos la capacidad de enviar correo electrónico de una cuenta, agregamos automáticamente el evento SES sending paused (Envío de SES suspendido) a la sección Event log (Registro de eventos) de PHD. El evento SES sending paused (Envío de SES suspendido) siempre tiene el estado Closed (Cerrado), independientemente de que actualmente esté suspendida o no la capacidad de la cuenta para enviar correo electrónico. El registro de eventos también incluye una copia del correo electrónico que enviamos a la dirección de correo electrónico asociada a tu AWS cuenta cuando se produjo la pausa en el envío.

Puede utilizarla CloudWatch para crear alarmas que le avisen cuando aparezcan nuevos eventos en su Personal Health Dashboard. Para obtener más información, consulte Supervisión de AWS Health eventos con CloudWatch eventos en la Guía del AWS Health usuario.

P4. Se ha suspendido la capacidad de mi cuenta para enviar correo electrónico. ¿Esto afecta a mi capacidad de usar otros AWS servicios?

Puedes seguir utilizando otros AWS servicios mientras la capacidad de tu cuenta para enviar correos electrónicos esté en pausa. Sin embargo, si solicita un aumento de la cuota de servicio para otro servicio de AWS que envíe comunicaciones de salida (como Amazon SNS), podríamos denegar dicha solicitud hasta que se restablezca la capacidad de su cuenta para enviar correo electrónico.

P5. ¿Qué debo hacer si la capacidad de mi cuenta para enviar correo electrónico se suspende?

Debe hacer lo siguiente:

- Consulte el correo electrónico que le hemos enviado para conocer un resumen del problema.
- Investigue sus envíos para determinar qué aspectos de su envío han desencadenado específicamente el problema.
- Tras realizar los cambios que crea que resolverán el problema, inicie sesión en la AWS consola y vaya al Support Center. Responda al caso que abrimos en su nombre. En su mensaje, proporcione información detallada sobre las medidas que ha tomado para resolver el problema y explique de qué manera estos pasos evitarán que el problema vuelva a producirse en el futuro.
- Asegúrese de facilitar toda la información que le solicitemos específicamente. Necesitamos esta información para evaluar su caso.

P6. ¿Qué es una revisión?

Puede solicitar que consideremos nuestra decisión de poner su cuenta en proceso de revisión. Consulte la siguiente pregunta para obtener más información sobre cómo solicitar una revisión.

P7. ¿Cómo puedo solicitar una revisión?

Para solicitar una revisión, inicie sesión en la AWS consola y vaya al Support Center. Responda al caso que abrimos en su nombre.

En la solicitud, proporcione la siguiente información:

- Información sobre lo que ha provocado el problema.
- Una lista de los cambios que ha realizado para corregir el problema. Incluya solo los pasos que ya ha implementado, no los que piensa implementar en el futuro.

- Información sobre cómo estos cambios evitarán que el mismo problema se repita en el futuro.

Dependiendo de la naturaleza del evento por el que suspendimos la capacidad de su cuenta para enviar correo electrónico, podríamos solicitar información adicional. Consulte el tema de las preguntas frecuentes relacionado con el problema que tuvo para obtener una lista de la información que debe incluir en la solicitud.

P8. ¿Qué ocurre si no se acepta mi solicitud?

Responderemos a su solicitud con información acerca de por qué no la hemos aceptado. En algunos casos, podrá enviar otra solicitud si puede demostrar que ha resuelto el problema, y que los cambios evitarán que el problema se repita en el futuro.

P9. ¿Puede ayudarme a diagnosticar el problema?

Normalmente podemos facilitarle solo información general de alto nivel sobre su problema (por ejemplo, que tiene un problema de rebotes). Es su responsabilidad corregir el problema.

P10. ¿Cómo puedo saber si la capacidad de mi cuenta para enviar correo electrónico se ha restablecido?

Las métricas de reputación incluyen información acerca del estado actual de su cuenta. Para obtener más información, consulte Uso de métricas de reputación para realizar un seguimiento de las tasas de rebotes y de reclamos.

P11. ¿Puedo obtener ayuda de mi AWS representante o de Premium Support?

Si ya estás trabajando con un representante de AWS cuentas, nos pondremos en contacto con él automáticamente si suspendemos la capacidad de tu cuenta para enviar correos electrónicos. Su representante de cuenta podría facilitarle información adicional para ayudarle a comprender mejor el problema. Si utiliza Premium Support, también debería ponerse en contacto con dicho equipo para obtener más ayuda.

Preguntas frecuentes sobre rebotes

Q1 (P1). ¿Por qué se preocupan por mis rebotes?

A menudo, los proveedores de correo electrónico y las organizaciones antispam utilizan las altas tasas de rebote para detectar a los remitentes con malas prácticas de envío de correo electrónico.

Las altas tasas de rebote pueden provocar que el correo electrónico se envíe a la carpeta de spam en lugar de a la bandeja de entrada.

Q2 (P2). ¿Qué debo hacer si recibo una notificación que indica que mi cuenta está en proceso de revisión o que mis envíos se han suspendido debido a la tasa de rebotes de mi cuenta?

Identifique la causa del problema y, a continuación, corríjala. Tras realizar los cambios que crea que resolverán el problema, inicie sesión en la AWS consola y vaya al Support Center. Responda al caso que abrimos en su nombre. En su mensaje, proporcione información detallada sobre las medidas que ha tomado para resolver el problema y explique de qué manera estos pasos evitarán que el problema vuelva a producirse en el futuro. Incluya también la información siguiente:

- El método que utiliza para realizar un seguimiento de sus rebotes
- Cómo se asegura de que las direcciones de correo electrónico de nuevos destinatarios sean válidas antes de enviarles mensajes. Por ejemplo, cual de las recomendaciones está siguiendo en P11. ¿Qué puedo hacer para minimizar los rebotes?

Q3 (P3). ¿Qué tipos de rebotes se contabilizan en mi tasa de rebotes?

Su tasa de rebotes solo incluye rebotes permanente a los dominios que no haya verificado. Los rebotes permanentes son errores de entrega permanentes como, por ejemplo, "la dirección no existe". Los errores temporales e intermitente, tales como "bandeja de entrada llena" o los rebotes debidos a direcciones IP bloqueadas, no se contabilizan en la tasa de rebotes.

P4. ¿Cuáles son las tasas de rebotes que podrían provocar que mi cuenta se coloque en proceso de revisión o que podrían provocar la suspensión de mis envíos?

Para obtener los mejores resultados, debe mantener una tasa de rebotes por debajo del 2 %. Las tasas de rebotes más altas pueden afectar a la entrega de sus correos electrónicos.

Si su tasa de rebotes es del 5 % o superior, pondremos su cuenta en proceso de revisión. Si su tasa de rebotes es del 10 % o superior, podríamos suspender la capacidad de su cuenta para enviar correo electrónico adicional hasta que resuelva el problema que ha dado como resultado la tasa elevada de rebotes.

P5. ¿Para qué periodo de tiempo se calcula mi tasa de rebotes?

No calcular la tasa de rebotes en función de un periodo de tiempo fijo, ya que distintos remitentes envían a ritmos diferentes. En lugar de ello, nos fijamos en un volumen representativo una cantidad de correo electrónico que representa sus prácticas de envío habituales. Para ser justos con los remitentes de volúmenes grandes y pequeños, el volumen representativo es distinto para cada usuario y cambia a medida que cambian los patrones de envío del usuario.

P6. ¿Puedo calcular mi propia tasa de rebote utilizando la información de la consola de SES o de la GetSendStatistics API?

No. La tasa de rebotes se calcula mediante el volumen representativo (consulte P5. ¿Para qué periodo de tiempo se calcula mi tasa de rebotes?). En función de la tasa de envíos, la tasa de rebote puede extenderse más atrás en el tiempo de lo que la consola de SES `GetSendStatistics` puede recuperar o recuperar. Además, solo los mensajes de correo electrónico a dominios verificados se tienen en cuenta a la hora de calcular la tasa de rebotes. No obstante, si monitoriza periódicamente su tasa de rebotes utilizando dichos métodos, debería tener un buen indicador que puede utilizar para identificar problemas antes de alcancen niveles que den lugar a que pongamos su cuenta en proceso de revisión o a que suspendamos la capacidad de su cuenta para enviar correo electrónico.

P7. ¿Cómo puedo averiguar qué direcciones de correo electrónico han presentado rebotes?

Examine las notificaciones de rebote que le envía SES. La dirección de correo electrónico a la que SES reenvía las notificaciones depende de cómo haya enviado los mensajes originales, tal y como se describe en. Recepción de notificaciones de Amazon SES por correo electrónico También puede configurar las notificaciones de rebotes mediante de Amazon Simple Notification Service (Amazon SNS), tal como se describe en Configuración de las notificaciones de eventos para Amazon SES. Tenga en cuenta que solo con eliminar de la lista las direcciones que presentan rebotes sin una investigación adicional podría no resolver el problema subyacente. Para obtener información acerca de lo que puede hacer para reducir los rebotes, consulte P11. ¿Qué puedo hacer para minimizar los rebotes?.

P8. Si yo no he monitorizado los rebotes, ¿pueden facilitarme una lista de las direcciones con rebote?

No, no podemos proporcionar una lista completa de las direcciones con rebote. El cliente es responsable de monitorizar y actuar en función de los rebotes de su cuenta.

P9. ¿Cómo debería gestionar los rebotes?

Tiene que eliminar las direcciones con rebotes de su lista de correo y dejar de enviarles correo electrónico de forma inmediata. Si es remitente de poco volumen, podría ser suficiente simplemente monitorizar los rebotes a través de correo electrónico y eliminar manualmente las direcciones con rebotes desde su lista de correo. Si el volumen es superior, probablemente desee configurar la automatización para este proceso, ya sea mediante programación procesando la bandeja de correo donde recibe los rebotes o configurando las notificaciones de rebote a través de Amazon SNS. Para obtener más información, consulte Configuración de las notificaciones de eventos para Amazon SES.

P10. ¿Podrían mis correos electrónicos rebotar por haber alcanzado mis cuotas de envío?

No. Los rebotes no están relacionados con las cuotas de envío. Si intentas superar tu cuota de envío, recibirás un error en la API o la interfaz SMTP de SES cuando intentes enviar un correo electrónico.

P11. ¿Qué puedo hacer para minimizar los rebotes?

En primer lugar, asegúrese de que estar al tanto de sus rebotes (consulte P7. ¿Cómo puedo averiguar qué direcciones de correo electrónico han presentado rebotes?). A continuación, siga estas instrucciones:

- No compre, alquile o comparta direcciones de correo electrónico. Envíe correo electrónico únicamente a los destinatarios que hayan solicitado de forma explícita recibir sus correos electrónicos.
- Elimine las direcciones de correo electrónico con rebote de su lista.
- En formularios web, pida a los usuarios que introduzcan sus direcciones de correo electrónico dos veces y asegúrese de que ambas direcciones coincidan antes de poder enviar el formulario.
- Utilice la confirmación doble para inscribir nuevos usuarios. Es decir, cuando un nuevo usuario se inscriba, envíele un correo electrónico de confirmación en el que sea preciso pulsar antes de recibir correo adicional. Esto evita que se inscriban a otras personas, así como las inscripciones accidentales.
- Si tiene que enviar mensajes a direcciones a las que no haya enviado últimamente (y, por lo tanto, no puede estar seguro de si las direcciones siguen siendo válidas), hágalo sólo con una pequeña parte de su envío general. Para obtener más información, consulte nuestro artículo de blog Never send to old addresses, but what if you have to?.

- Asegúrese de que las inscripciones no estén estructuradas de modo que anime a los usuarios a utilizar direcciones ficticias. Por ejemplo, no proporcione ningún valor añadido o beneficios hasta que los destinatarios verifiquen sus direcciones.
- Si dispone de una funcionalidad "enviar por correo electrónico a un amigo", utilice CAPTCHA o un mecanismo similar para impedir el uso automatizado de la misma y no permitir al usuario insertar contenido arbitrario.
- Si utilizas SES para las notificaciones del sistema, asegúrate de enviar las notificaciones a direcciones reales que puedan recibir correo. Considere además la posibilidad de desactivar las notificaciones que no necesita.
- Si está probando un sistema nuevo, asegúrese de enviar mensajes a direcciones reales que puedan recibir correos electrónicos o de utilizar el simulador de buzones de correo de SES. Para obtener más información, consulte Uso del simulador de buzón de correo de forma manual.

Preguntas frecuentes sobre reclamaciones

Q1 (P1). ¿Qué es una reclamación?

Una reclamación se produce cuando un destinatario notifica que no desea recibir un correo electrónico. Es posible que hayan hecho clic en el botón «Denunciar spam» de su cliente de correo electrónico, hayan presentado una queja a su proveedor de correo electrónico, hayan notificado directamente a SES o hayan utilizado algún otro método. En este tema se incluye información general sobre las reclamaciones. Si tu notificación contiene información específica sobre el origen de las quejas, lee también el tema correspondiente:

- Preguntas frecuentes sobre las quejas de SES a través de circuitos de retroalimentación
- Preguntas frecuentes sobre las quejas de SES directamente de los destinatarios
- Preguntas frecuentes sobre quejas de SES a través de proveedores de correo electrónico

Q2 (P2). ¿Por qué se preocupa por mis reclamaciones?

Entidades como, por ejemplo, los proveedores de correo electrónico y las organizaciones antispam suelen utilizar las tasas de reclamación elevadas como indicadores de que el remitente está enviando a destinatarios que no se han registrado específicamente para recibir mensajes de correo electrónico o que el remitente está enviando contenido distinto del tipo al que los destinatarios se han inscrito.

Q3 (P3). ¿Qué debo hacer si recibo una notificación que indica que mi cuenta está en proceso de revisión o que mis envíos se han suspendido debido a un problema con las reclamaciones?

Revise su proceso de adquisición de lista y el contenido de sus correos electrónicos para intentar comprender por qué sus destinatarios podrían no estar interesados en el correo electrónico que les está enviando. Identifique la causa del problema y, a continuación, corríjala. Tras realizar los cambios que crea que resolverán el problema, inicie sesión en la AWS consola y vaya al Support Center. Responda al caso que abrimos en su nombre. En su mensaje, proporcione información detallada sobre las medidas que ha tomado para resolver el problema y explique de qué manera estos pasos evitarán que el problema vuelva a producirse en el futuro.

P4. ¿Qué puedo hacer para minimizar las reclamaciones?

En primer lugar, asegúrese de supervisar las quejas que SES puede notificarle, que son quejas que SES recibe a través de circuitos de retroalimentación (consulte laPreguntas frecuentes sobre las quejas de SES a través de circuitos de retroalimentación). A continuación, siga estas instrucciones:

- No compre, alquile o comparta direcciones de correo electrónico. Utilice solo direcciones que hayan solicitado específicamente su correo electrónico.
- Utilice la confirmación doble para inscribir nuevos usuarios. Es decir, cuando un usuario se inscriba, envíele un correo electrónico de confirmación en el que sea preciso pulsar antes de recibir correo adicional. Esto evita que se inscriban a otras personas, así como las inscripciones accidentales.
- Monitorice la implicación de los usuarios con el correo electrónico que envía y deje de enviar mensajes a destinatarios que no abran o hagan clic en sus mensajes.
- Cuando se registran nuevos usuarios, indique con claridad el tipo de correo electrónico que les enviará y asegúrese de enviarles únicamente el tipo de correo electrónico en el que se hayan inscrito. Por ejemplo, si los usuarios se inscriben para actualizaciones de noticias, no les envíe anuncios.
- Asegúrese de que su correo electrónico tenga un formato correcto y un aspecto profesional.
- Asegúrese de que su correo electrónico proceda claramente de usted y no pueda confundirse con otras cosas.
- Proporcione a los usuarios una forma sencilla y obvia de cancelar la suscripción a su correo electrónico.

Preguntas frecuentes sobre las quejas de SES a través de circuitos de retroalimentación

En este tema se proporciona información sobre las quejas que SES recibe de los proveedores de correo electrónico a través de los circuitos de retroalimentación. Para obtener información general relativa a todos los tipos de reclamos, consulte Preguntas frecuentes sobre reclamaciones.

Q1 (P1). ¿Cómo se notifica este tipo de reclamo?

La mayoría de los programas cliente de correo electrónico ofrecen un botón "Marcar como spam", o similar, que traslada el mensaje a una carpeta de spam y lo reenvía al proveedor de correo electrónico. Además, la mayoría de los proveedores de correo electrónico mantienen una dirección de abuso (por ejemplo, abuse@example.com), donde los usuarios pueden reenviar correo electrónico no deseado y solicitar al proveedor que tome las medidas necesarias para evitarlos. Si SES tiene un circuito de retroalimentación (FBL) establecido con el proveedor de correo electrónico, este devolverá la queja a SES.

> **Note**
>
> SES establece automáticamente el encabezado Feedback-ID cuando envías los mensajes, lo que permite a los proveedores de buzones agregar estadísticas de entrega, como las tasas de quejas y spam, y ponerlas a tu disposición. El valor del encabezado Feedback-ID que proporciona SES se compone de la siguiente manera:
>
> - `FeedBackId:((SESInternalID):(AmazonSES))`, donde:
>   - SESInternalID es el identificador utilizado por SES para recopilar la información sobre las quejas.
>   - AmazonSES es una etiqueta estática que identifica a SES como la plataforma de envío.
>
> Si lo desea, además del valor de encabezado de ID de comentarios estándar que proporciona SES, también puede especificar sus propios ID de comentarios personalizados (hasta dos) utilizando las etiquetas `ses:feedback-id-a` y del `ses:feedback-id-b` mensaje (consulte). the section called “Comentarios detallados para las campañas de correo electrónico”

Q2 (P2). ¿Se incluyen estas quejas en la estadística del porcentaje de quejas que se muestra en la consola de SES y las devuelve la API? GetSendStatistics

Sí. Sin embargo, la estadística del porcentaje de quejas no incluye las quejas de los proveedores de correo electrónico que no envían comentarios a SES. La tasa de reclamaciones de dominios que proporcionan retroalimentación es probable que también sea representativa del resto de sus envíos.

Q3 (P3). ¿Cómo puedo recibir notificaciones sobre estas reclamaciones?

Puede recibir notificaciones a través de correo electrónico o a través de notificaciones de Amazon SNS. Vea las instrucciones de configuración en Configuración de las notificaciones de eventos para Amazon SES.

P4. ¿Qué debo hacer si recibo una notificación de reclamo a través de correo electrónico o a través de Amazon SNS?

En primer lugar, tiene que eliminar las direcciones que generen reclamaciones de su lista de correo y dejar de enviarles correo electrónico de forma inmediata. No envíe siquiera un correo electrónico que indique que ha recibido la solicitud para cancelar la suscripción. Sopese la posibilidad de configurar la automatización para este proceso, ya sea mediante programación procesando la bandeja de correo donde recibe los reclamos o configurando las notificaciones de reclamo a través de Amazon SNS. Para obtener más información, consulte Configuración de las notificaciones de eventos para Amazon SES.

A continuación, examine detenidamente sus envíos para determinar por qué los destinatarios no desean el correo que está enviando y aborde el problema subyacente. Por cada persona que reclama puede haber docenas que no desean su correo electrónico que no se quejan o no han podido hacerlo. Si lo único que hacer es eliminar los destinatarios que reclaman realmente, no aborda el problema subyacente.

P5. ¿Indican las tasas de quejas de SES que podrían provocar que mi cuenta fuera objeto de revisión o que podrían provocar una pausa en la capacidad de mi cuenta para enviar correos electrónicos?

Para obtener los mejores resultados, debe mantener una tasa de reclamaciones por debajo del 0,1 %. Las tasas de reclamos más altas pueden afectar a la entrega de sus correos electrónicos.

Si su tasa de reclamaciones es del 0,1 % o superior, pondremos su cuenta en proceso de revisión. Si su tasa de reclamaciones es del 0,5 % o superior, podríamos suspender la capacidad de su cuenta para enviar correo electrónico adicional hasta que resuelva el problema que ha dado como resultado la tasa elevada de reclamaciones.

P6. ¿Para qué periodo de tiempo se calcula mi tasa de reclamaciones?

No calcular la tasa de reclamaciones en función de un periodo de tiempo fijo, ya que distintos remitentes envían a ritmos diferentes. En lugar de ello, nos fijamos en un volumen representativo: una cantidad de correo que representa sus prácticas de envío típicas. Para ser justos con los remitentes de volúmenes grandes y pequeños, el volumen representativo es distinto para cada usuario y cambia a medida que cambian los patrones de envío del usuario. Además, la tasa de reclamaciones no se calcula en función de cada mensaje de correo electrónico. En cambio, se calcula como el porcentaje de quejas en el correo enviado a los dominios que envían comentarios sobre las quejas a SES.

P7. ¿Puedo calcular mi propio porcentaje de quejas utilizando las métricas de la consola de SES o de la GetSendStatistics API?

No. Existen dos razones principales para ello:

- La tasa de reclamaciones se calcula mediante el volumen representativo (consulte P6. ¿Para qué periodo de tiempo se calcula mi tasa de reclamaciones?). En función de su tasa de envíos, su tasa de quejas puede extenderse más atrás en el tiempo de lo que la consola o la `GetSendStatistics` API de SES pueden recuperar. Por este motivo, le recomendamos que utilice a menudo estos métodos para monitorizar la tasa de reclamaciones de su cuenta. La monitorización de la tasa de reclamaciones de esta forma le ofrece la información que necesita para identificar problemas antes de que alcancen niveles que podrían afectar a la entrega de su correo electrónico.
- Para calcular la tasa de reclamaciones, no se contabilizan todos los correos electrónicos. La tasa de quejas se calcula como el porcentaje de quejas por correo que se envían a los dominios que envían comentarios sobre las quejas a SES.

P8. ¿Cómo puedo averiguar qué direcciones de correo electrónico han presentado reclamos?

Examine las notificaciones de quejas que SES le envía por correo electrónico o a través de Amazon SNS (consulteConfiguración de las notificaciones de eventos para Amazon SES). Sin embargo, los distintos proveedores de correo electrónico proporcionan diferentes cantidades de información y algunos proveedores ocultan la dirección de correo electrónico del destinatario antes de enviar la notificación de queja a SES. Para que pueda encontrar la dirección de correo electrónico del destinatario en el futuro, la mejor opción es almacenar su propio mapeo entre un identificador y el ID del mensaje de SES que SES le devuelve cuando acepta el correo electrónico. Tenga en cuenta que SES no conserva ningún identificador de mensaje personalizado que usted añada.

P9. En caso de no haber monitorizado mis reclamaciones, ¿pueden facilitarme una lista de las direcciones con reclamaciones?

Lamentablemente, no podemos proporcionarle una lista exhaustiva. Sin embargo, puede monitorear reclamos futuros por correo electrónico o a través de Amazon SNS.

P10. ¿Puedo obtener un correo electrónico de muestra?

No podemos enviarle un correo electrónico de muestra previa petición, pero es posible encontrar esta información en la notificación de la reclamación. Para obtener más información, consulte P8. ¿Cómo puedo averiguar qué direcciones de correo electrónico han presentado reclamos?.

Preguntas frecuentes sobre las quejas de SES directamente de los destinatarios

Este tema proporciona información sobre las quejas que SES recibe directamente de los destinatarios. Para obtener información general relativa a todos los tipos de reclamos, consulte Preguntas frecuentes sobre reclamaciones.

Q1 (P1). ¿Cómo se notifica este tipo de reclamo?

Varios destinatarios se pusieron en contacto directamente con SES en relación con su correo electrónico o por algún otro medio.

Q2 (P2). ¿Se incluyen estas quejas en la estadística del porcentaje de quejas que se muestra en la consola de SES y las devuelve la GetSendStatistics API?

No. La estadística del porcentaje de quejas que obtiene mediante la consola o la `GetSendStatistics` API de SES solo incluye las quejas que SES recibe a través de bucles de retroalimentación. Para obtener más información acerca de estos tipos de reclamaciones, consulte Preguntas frecuentes sobre las quejas de SES a través de circuitos de retroalimentación.

Q3 (P3). ¿Por qué no he oído hablar de estos reclamos a través de notificaciones de retroalimentación de correo electrónico o a través de Amazon SNS?

El reenvío de comentarios por correo electrónico y las notificaciones de Amazon SNS solo incluyen las quejas que SES recibe a través de los bucles de comentarios. No recibirás notificaciones de las quejas que los destinatarios hayan presentado directamente a SES.

P4. ¿Cómo puedo averiguar qué direcciones de correo electrónico han presentado reclamos?

Para proteger las identidades de los destinatarios que se han quejado, no podemos enumerar las direcciones de correo electrónico que han presentado una reclamación por su correo electrónico.

En lugar de centrarse en eliminar destinatarios individuales de sus listas, le recomendamos que determine el problema que ha llevado a la formulación de las reclamaciones. Le recomendamos que empiece por revisar el proceso de adquisición de clientes y que retire de sus listas a aquellos que no hayan solicitado explícitamente recibir sus correos electrónicos. También debe analizar el contenido de sus correos electrónicos para intentar comprender por qué se han quejado los destinatarios.

P5. ¿Puedo obtener un correo electrónico de muestra?

Para proteger las identidades de los destinatarios que se han quejado, no podemos proporcionarle copias de los correos electrónicos que han provocado que los destinatarios se quejen.

P6. ¿Qué debo hacer si recibo una notificación que indica que mi cuenta está en proceso de revisión o que mis envíos se han suspendido debido a reclamaciones directas?

Inmediatamente cambie los procesos de envío, de modo que solo envíe mensajes a destinatarios que se hayan inscrito específicamente para recibirlos. Además, asegúrese de que está enviando el tipo de contenido al que los destinatarios se registraron para recibir. Tras realizar los cambios que crea que resolverán el problema, inicie sesión en la AWS consola y vaya al Support Center. Responda al caso que abrimos en su nombre. En su mensaje, proporcione información detallada sobre las medidas que ha tomado para resolver el problema y explique de qué manera estos pasos evitarán que el problema vuelva a producirse en el futuro.

Si no solicita una revisión en un plazo de tres semanas y seguimos recibiendo reclamaciones directas de los destinatarios, podríamos suspender la capacidad de su cuenta para enviar correo electrónico.

Preguntas frecuentes sobre quejas de SES a través de proveedores de correo electrónico

En este tema se proporciona información sobre las quejas que SES recibe a través de los proveedores de correo electrónico (también denominados proveedores de buzones de correo). Para obtener información general relativa a todos los tipos de reclamos, consulte Preguntas frecuentes sobre reclamaciones.

Q1 (P1). ¿Cómo se notifica este tipo de reclamo?

Un proveedor de correo electrónico informó a SES de que un número significativo de sus clientes marcaba sus correos electrónicos como spam. El informe se proporcionó a SES a través de un medio distinto de los circuitos de retroalimentación descritos en elPreguntas frecuentes sobre las quejas de SES a través de circuitos de retroalimentación.

Q2 (P2). ¿Se incluyen estas quejas en la estadística del porcentaje de quejas que se muestra en la consola de SES y las devuelve la GetSendStatistics API?

No. La estadística del porcentaje de quejas que obtiene mediante la consola o la `GetSendStatistics` API de SES solo incluye las quejas que SES recibe a través de bucles de retroalimentación.

Q3 (P3). ¿Por qué no he oído hablar de estos reclamos a través de notificaciones de retroalimentación de correo electrónico o a través de Amazon SNS?

El reenvío de comentarios por correo electrónico y las notificaciones de Amazon SNS solo incluyen las quejas que SES recibe a través de los bucles de comentarios.

P4. ¿Cómo puedo averiguar qué direcciones de correo electrónico han presentado reclamos?

Los proveedores de correo electrónico normalmente no revelan esta información. Sin embargo, en lugar de centrarse en eliminar destinatarios individuales de la lista, debe centrarse en encontrar y solucionar el problema subyacente. Empiece por revisar su proceso de adquisición de lista y el contenido de sus correos electrónicos para intentar comprender por qué sus destinatarios podrían no estar interesados en su correo electrónico.

P5. ¿Puedo obtener un correo electrónico de muestra?

No. Los proveedores de correo electrónico normalmente no proporcionan un correo electrónico de ejemplo.

P6. ¿Qué debo hacer si recibo una notificación que indica que mi cuenta está en proceso de revisión o que mis envíos se han suspendido debido a reclamaciones de los proveedores de correo electrónico?

Identifique la causa del problema y, a continuación, corríjala. Tras realizar los cambios que crea que resolverán el problema, inicie sesión en la AWS consola y vaya al Support Center. Responda al caso que abrimos en su nombre. En su mensaje, proporcione información detallada sobre las medidas que ha tomado para resolver el problema y explique de qué manera estos pasos evitarán que el problema vuelva a producirse en el futuro. Si no solicita una revisión en un plazo de tres semanas y seguimos recibiendo reclamaciones de los proveedores, podríamos suspender la capacidad de su cuenta para enviar correo electrónico adicional.

Preguntas frecuentes sobre trampas de spam

Q1 (P1). ¿Qué son las trampas de spam?

Una trampa de spam es una dirección de correo electrónico especial mantenida por un proveedor de Internet (ISP), un proveedor de correo electrónico o una organización antispam. Dado que esa dirección no se inscribirá nunca de manera legítima para recibir correo electrónico, las organizaciones que mantener estas trampas de spam saben que quien envía a cualquiera de estas direcciones de correo electrónico probablemente siga prácticas de correo electrónico cuestionables.

Q2 (P2). ¿Cómo se configuran las trampas de spam?

Las direcciones de trampa de spam se pueden configurar de varias formas. Se pueden convertir a partir de direcciones que anteriormente fueron válidas, pero que han dejado de utilizarse (y de rebotar) durante un periodo de tiempo prolongado. También pueden ser direcciones que configuraron para ser trampas de spam. Pueden ser direcciones inusuales que sean difíciles de adivinar y, en ocasiones, son direcciones parecidas a direcciones reales (por ejemplo, introducen una errata en un nombre de dominio común). A menudo, pero no siempre, las trampas de spam se "siembran" en el mundo colocándolas en Internet de diversas formas.

Q3 (P3). ¿Cómo sabe SES si estoy enviando mensajes a las trampas de spam?

Algunas organizaciones que utilizan trampas de spam envían notificaciones a SES cuando sus trampas de spam son atacadas por remitentes de SES.

P4. ¿Cómo utiliza SES los informes sobre las trampas de spam?

Nosotros revisamos los informes. Si determinamos que su cuenta está enviando correo electrónico a trampas de spam, ponemos su cuenta en proceso de revisión y le pedimos que corrija el problema subyacente. Si no corrige el problema antes de que finalice el periodo de revisión, podríamos suspender la capacidad de su cuenta para enviar correo electrónico adicional. Si su problema de trampa de spam es muy grave, podríamos suspender la capacidad de su cuenta para enviar correo electrónico de forma inmediata, sin poner su cuenta primero en proceso de revisión.

P5. ¿Qué debo hacer si recibo una notificación que indica que mi cuenta está en proceso de revisión o que mis envíos se han suspendido debido a un problema con las trampas de spam?

En primer lugar, debe solucionar el problema que hizo que pusiéramos su cuenta en proceso de revisión o que suspendiéramos su capacidad para enviar correo electrónico. A continuación, inicie

sesión en la AWS consola y vaya al Support Center. Responda al caso que abrimos en su nombre. En su mensaje, proporcione información detallada sobre las medidas que ha tomado para resolver el problema y explique de qué manera estos pasos evitarán que el problema vuelva a producirse en el futuro. Si estamos de acuerdo en que los cambios que ha realizado solucionan el problema de forma adecuada, cancelaremos el periodo de revisión o eliminaremos la suspensión del envío desde su cuenta.

Debido a la forma en que se notifican las incidencias de las trampas de spam, pueden ser necesarias tres semanas o más para que podamos determinar si los cambios que ha realizado resuelven el problema.

P6. ¿Cuántas incidencias de trampas de spam puedo tener antes de que se ponga mi cuenta en proceso de revisión o se suspenda la capacidad de mi cuenta para enviar correo electrónico?

No revelamos el número específico de incidencias de trampas de spam que hacen que actuemos en una cuenta. Sin embargo, es importante tener en cuenta que incluso un pequeño número de incidencias de trampas de spam puede tener un efecto muy negativo en su reputación como remitente, por lo que se debe tomar en serio los informes de trampas de spam.

P7. ¿Revela las direcciones de trampa de spam?

No. Para que las trampas de spam sean eficaces, es esencial que sigan siendo confidenciales. Las organizaciones de trampas de spam solo revelan el uso de las trampa de spam, no las direcciones de trampa de spam reales.

P8. ¿Qué puedo hacer para evitar el envío a trampas de spam?

Para reducir el riesgo de enviar a trampas de spam, siga estas directrices:

- No compre, alquile o comparta direcciones de correo electrónico. Utilice solo direcciones que hayan solicitado específicamente su correo electrónico.
- En formularios web, pida a los usuarios que introduzcan sus direcciones de correo electrónico dos veces y asegúrese de que ambas direcciones coincidan antes de poder enviar el formulario.
- Utilice la confirmación doble para inscribir nuevos usuarios. Es decir, cuando un usuario se inscriba, envíele un correo electrónico de confirmación en el que sea preciso pulsar antes de recibir correo adicional.
- Asegúrese de eliminar de su lista las direcciones con rebotes permanentes, para que se eliminen mucho antes de que se convierten en trampas de spam.

- Asegúrese de monitorizar la implicación de sus destinatarios y deje de enviar mensajes a destinatarios que no hayan interactuado recientemente con sus mensajes de correo electrónico o sitio web. Los plazos que determinan qué es un "usuario implicado" dependen del caso de uso, pero en general si los usuarios no han abierto sus mensajes de correo electrónico o hecho clic en ellos desde hace meses, debería plantearse eliminarlos a menos que haya pruebas de que desean su correo.
- Tenga mucho cuidado con las campañas para volver a implicar a usuarios en las que se ponga en contacto de manera intencionada con personas que no hayan interactuado con usted recientemente. Estos esfuerzos suelen ser muy arriesgados y, a menudo, puede causar problemas no solo con el envío de trampas de spam, sino también con el correo devuelto y las reclamaciones.
- Envíe un mensaje para darse de alta a toda su lista de correo y mantenga solo los destinatarios que hayan hecho clic en el enlace de verificación. Además de eliminar los destinatarios inactivos de la lista, este procedimiento también ayuda a eliminar las direcciones de trampas de spam. Sin embargo, no le recomendamos utilizar esta técnica si cree que su lista de correo podría contener muchas direcciones incorrectas o si su cuenta ya ha tenido un problema con los rebotes, ya que podría hacer que la tasa de rebotes de su cuenta aumente aún más.

Preguntas frecuentes sobre investigaciones manuales

Q1 (P1). ¿Qué debo hacer si recibo una notificación que indica que mi cuenta está en proceso de revisión o que mis envíos se han suspendido debido a una investigación manual?

Un investigador del SES ha identificado un problema importante con su envío. Entre los problemas típicos se incluyen, entre otros, los siguientes:

- Su envío infringe la Política de uso aceptable de AWS (AUP).
- Su correos electrónicos parecen no haber sido solicitados.
- Tu contenido está relacionado con una actividad de suplantación de identidad (esto incluye suplantación de identidad simulada).
- Por lo demás, su contenido está asociado a un caso de uso que SES no admite.

Si creemos que el problema puede corregirse, ponemos su cuenta en proceso de revisión durante un periodo de tiempo determinado. Mientras su cuenta esté en proceso de revisión, debe realizar cambios en sus prácticas de envío de correo electrónico para corregir el problema.

Si no creemos que el problema pueda corregirse, o si el problema es muy grave, podríamos suspender la capacidad de su cuenta para enviar correo electrónico sin ponerla antes en proceso de revisión.

Q2 (P2). ¿Qué problemas podrían provocar una revisión manual de mi envío de correo electrónico?

Hay varios problemas que podrían hacer que iniciemos una revisión manual de su cuenta. Entre otras, se incluyen las razones siguientes:

- Los destinatarios se ponen en contacto con SES para presentar una queja sobre el correo electrónico enviado desde su cuenta.
- Hemos detectado cambios inusuales en sus patrones de envío de correo electrónico.
- Nuestros filtros de spam encuentran características en su correo electrónico que son típicas del contenido no solicitado o de baja calidad.

Cuando pongamos su cuenta en proceso de revisión o suspendamos la capacidad de su cuenta para enviar correo electrónico, le enviaremos una notificación. En la mayoría de los casos, esta notificación contiene información sobre el problema y proporciona información sobre los siguientes pasos que puede realizar.

Q3 (P3). ¿Qué son los correos electrónicos "no solicitados"?

Los correos electrónicos no solicitados son correos electrónicos que el destinatario no ha solicitado recibir de forma explícita. Esto incluye los casos en que un destinatario se inscribe para un determinado tipo de correo (por ejemplo, notificaciones) y en su lugar se envía otro tipo de correo electrónico (por ejemplo, anuncios).

Cuando pongamos su cuenta en proceso de revisión o suspendamos la capacidad de su cuenta para enviar correo electrónico, le enviaremos una notificación. Si recibe una notificación en la que se indica que estamos tomando una de estas medidas debido a un problema con el correo electrónico no solicitado, inicie sesión en la AWS consola y vaya al Support Center. Responda al caso que abrimos en su nombre. El mensaje, incluya la siguiente información:

- ¿Todos los mensajes que envía han sido solicitados específicamente por el destinatario y se ajustan a la Política de uso aceptable de AWS?

- ¿Ha adquirido las direcciones de correo electrónico de alguna forma distinta a que el cliente interactúe específicamente con usted o su sitio web y le haya solicitado los correos electrónicos? Debe explicar cómo ha adquirido su lista de correo.
- ¿Cómo funcionan sus procesos de suscripción y cancelación de la suscripción? Debe incluir sus enlaces de inscripción y cancelación.

P4. ¿Qué debo hacer si recibo una notificación que indica que mi cuenta está en proceso de revisión o que mis envíos se han suspendido debido a una revisión manual?

Identifique la causa del problema y, a continuación, corríjala. Tras realizar los cambios que crea que resolverán el problema, inicie sesión en la AWS consola y vaya al Support Center. Responda al caso que abrimos en su nombre. En su mensaje, proporcione información detallada sobre las medidas que ha tomado para resolver el problema y explique de qué manera estos pasos evitarán que el problema vuelva a producirse en el futuro. Si estamos de acuerdo en que los cambios que ha realizado solucionan el problema de forma adecuada, cancelaremos el periodo de revisión de su cuenta.

P5. ¿Qué tipos de problemas ve como "subsanables?"

En general, creemos que la situación es subsanable si tiene un historial de buenas prácticas de envío y si hay medidas que puede adoptar para eliminar el envío problemático y, al mismo tiempo, continuar con la mayoría de envío. Por ejemplo, si envía tres tipos distintos de correo electrónico y solo uno de ellos es problemático, es posible que pueda simplemente detener el envío problemático y continuar con el resto de su envío.

P6. ¿Qué sucede si no puedo encontrar el origen del problema?

Puede iniciar sesión en la AWS consola e ir al Support Center. Responda al caso que hemos abierto en su nombre y solicite una muestra del correo electrónico que ha provocado el problema.

Preguntas frecuentes acerca de la lista de agujeros negros de DNS (DNSBL)

Listas de agujeros negros basadas en el sistema de nombres de dominio (DNSBL): también conocidas como Listas de agujeros negros en tiempo real (RBL), listas de denegación, listas

de bloqueo o listas negras, estas listas informan a los proveedores de correo electrónico sobre direcciones IP que se consideran sospechosas de enviar correo electrónico no deseado.

Cada una de estas DNSBL afectan de forma diferente a la capacidad de entrega de correo electrónico. Este tema describe el impacto de las DNSBL en la entrega de correos electrónicos enviados con Amazon SES, así como las políticas para eliminar direcciones IP de Amazon SES de las DNSBL.

> **Note**
>
> Este tema trata de las DNSBL que utilizan los proveedores de correo electrónico para bloquear los mensajes entrantes. Para obtener información acerca de cómo bloquea Amazon SES el correo electrónico saliente enviado a destinatarios cuyas direcciones de correo electrónico han generado rebotes anteriormente, consulte Lista de supresión global de Amazon SES.

P1. ¿Cómo afectan las DNSBL a la entrega de correo electrónico?

Cada una de estas DNSBL afecta de forma diferente a la capacidad de entrega correcta de los mensajes. Los principales proveedores de correo electrónico, como, por ejemplo, Gmail, Hotmail, AOL y Yahoo, reconocen un número muy reducido de DNSBL de gran confianza, como las que ofrece Spamhaus. Según nuestra experiencia, otras DNSBL no suelen tener un impacto importante, aunque algunos sistemas de correo electrónico dan preferencia a determinadas DNSBL sobre otras.

Por último, muchos proveedores de correo electrónico tienen sus propias listas de denegación internas. Los proveedores de correo electrónico guardan estas listas muy celosamente y en contadas ocasiones las comparten con el público. Si una dirección IP está en una de estas listas, puede tener un impacto importante en la capacidad de enviar correo electrónico a destinatarios que utilizan ese proveedor.

P2. ¿Cómo terminan las direcciones IP en las DNSBL?

Hay varias maneras en las que una dirección IP puede terminar en una DNSBL. Las direcciones IP se pueden agregar a DNSBL cuando envían correo electrónico a una trampa de spam. Una trampa de spam es una dirección de correo electrónico que no pertenece a un usuario humano. Su único propósito es recopilar spam e identificar a los spammers. Algunas DNSBL también permiten a los usuarios individuales enviar direcciones IP. Algunas DNSBL incluso permiten a los usuarios

enviar rangos de direcciones IP completos. Otras DNSBL se mantienen mediante contribuciones de administradores de correo electrónico y pueden incluir direcciones IP que los administradores sospechan que están abusando de sus propios sistemas.

P3. ¿Cómo evita Amazon SES que sus direcciones IP aparezcan en DNSBL?

Nuestros sistemas buscan signos de abuso. Si detectamos patrones de envío u otras características que podrían ocasionar la inclusión de una dirección IP en una DNSBL, enviamos una notificación al remitente. Si la situación es grave, o si el remitente no soluciona el problema tras recibir la notificación, suspenderemos su capacidad para enviar mensajes de correo electrónico hasta que resuelva el problema. Esta manera de aplicar nuestras políticas de envío ayuda a reducir las posibilidades de que nuestras direcciones IP acaben incluidas en DNSBL.

P4. ¿Puede quitar Amazon SES sus direcciones IP de una DNSBL?

Monitoreamos de forma activa las DNSBL que podrían afectar a la entrega en todo el servicio de Amazon SES o la capacidad de enviar correo electrónico a destinatarios que utilizan alguno de los principales proveedores de correo electrónico, como, por ejemplo, Gmail, Yahoo, AOL y Hotmail. Las DNSBL que ofrece Spamhaus pertenecen a esta categoría. Si una de nuestras direcciones IP aparece en una lista que cumple alguno de estos criterios, tomamos medidas de inmediato para que se elimine la dirección de la DNSBL lo antes posible.

No monitoreamos DNSBL que tienen pocas probabilidades de afectar a la entrega en todo el servicio de Amazon SES, o que no tienen un impacto cuantificable en la entrega a los principales proveedores de correo electrónico. Las DNSBL que ofrecen SORBS y UCEPROTECT pertenecen a esta categoría. Debido a las prácticas específicas de inclusión y eliminación de los proveedores que operan estas listas, no podemos eliminar nuestras direcciones IP de estas listas.

P5. Un proveedor de correo electrónico rechaza mi correo electrónico porque la dirección IP de envío aparece en una DNSBL distinta de Spamhaus. ¿Qué puedo hacer?

En primer lugar, confirme que el mensaje se bloqueó realmente debido a una DNSBL. Si el correo electrónico se rechazó porque la dirección IP de envío estaba en una DNSBL, recibirá una notificación de rebote que menciona el nombre del proveedor de DNSBL, como en el ejemplo siguiente:

```
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 ha recibido una notificación de rebote, pero esta no contenía información similar a la del mensaje mostrado en el ejemplo anterior, lo más probable es que el proveedor de correo electrónico haya rechazado su mensaje por un motivo no relacionado con las DNSBL.

Si puede confirmar que un proveedor de correo electrónico está bloqueando su correo electrónico porque la dirección IP de envío aparece en una DNSBL, hay varias cosas que puede hacer:

- Póngase en contacto con el administrador de correo del dominio que rechazó su mensaje para solicitarle que haga una excepción en su política de filtrado de spam. Algunos administradores de correo disponen de procesos de soporte y es posible que publiquen una página para administradores de correo que describa este proceso. Si el dominio con el que intenta ponerse en contacto no publica sus políticas de soporte para administradores de correo, es posible que pueda ponerse en contacto con el administrador de correo enviando un correo electrónico a postmaster@*example.com*, donde *example.com* es el dominio en cuestión. La especificación RFC 5321 requiere que los dominios tengan un buzón para administradores de correo.

  Cuando contacte con el administrador de correo, facilite los códigos de rebote que ha recibido, los encabezados del correo que intenta enviar, una medida del impacto que tiene la DNSBL en la entrega de su correo e información acerca de por qué cree que se está bloqueando incorrectamente su correo. Cuanta más información pueda proporciona al administrador de correo para demostrar que está enviando correo electrónico legítimo, más probable será que el administrador haga una excepción con usted.
- Si el proveedor de correo electrónico no responde, o no está dispuesto cambiar sus políticas, considere la posibilidad de utilizar una dirección IP dedicada. Las direcciones IP dedicadas son direcciones que solo usted puede utilizar. La implementación de buenas prácticas de envío le permitirá mantener sus índices de aceptación altos, y las tasas de rebotes, reclamaciones y trampas de spam bajas. Estas prácticas pueden ayudarle a garantizar que sus direcciones no acabarán en DNSBL.

P6. El correo electrónico que envío a Gmail, Yahoo, Hotmail u otro proveedor importante se envía a la carpeta de spam. ¿Esto sucede porque mi dirección IP de envío está en una DNSBL?

Probablemente no. Si una dirección IP aparece en una DNSBL con un impacto significativo, como una de las DNSBL de Spamhaus, los principales proveedores de correo electrónico rechazarán el correo electrónico de esa dirección IP, en lugar de enviarlo a la carpeta de spam.

Cuando los principales proveedores de correo electrónico aceptan correo (en lugar de rechazarlo), normalmente tienen en cuenta la interacción de los usuarios a la hora de determinar si deben colocar el mensaje en la bandeja de correo o en la carpeta de spam. La interacción de los usuarios hace referencia a las formas en que los usuarios interactuaron con los mensajes que les envió anteriormente.

Para aumentar las posibilidades de que sus mensajes lleguen a la bandeja de entrada de sus clientes, debería implementar todas las prácticas recomendadas siguientes:

- No alquile o compre listas de correo electrónico. El alquiler o la compra de listas es una infracción de la Política de uso aceptable de AWS (AUP) y no están permitidos en Amazon SES bajo ninguna circunstancia.
- Envíe correo electrónico solo a los clientes que hayan solicitado de forma explícita recibir sus correos electrónicos. En muchos países y jurisdicciones de todo el mundo, es ilegal enviar correo electrónico a destinatarios que no acepten explícitamente recibir correo electrónico de usted.
- Deje de enviar mensajes de correo electrónico a clientes que no hayan abierto o hecho clic en los enlaces de los mensajes que haya enviado en los últimos 30-90 días. Este paso puede ayudar a mantener sus tasas de interacción altas, lo que aumenta las posibilidades de que los mensajes que envíe en el futuro lleguen a las bandejas de entrada de los destinatarios.
- Utilice elementos de diseño y estilos de redacción coherentes en cada mensaje que envíe para asegurarse de que los clientes puedan identificar fácilmente sus mensajes.
- Utilice mecanismos de autenticación de correo electrónico, como SPF y DKIM.
- Cuando los clientes utilicen un formulario web para suscribirse a su contenido, envíeles un correo electrónico para confirmar que desean recibir correo electrónico. No les envíe ningún correo electrónico más hasta que confirmen que desean recibir su correo electrónico. Este proceso se conoce como activación confirmada o doble activación.
- Facilite a sus clientes la cancelación de las suscripciones y acepte las solicitudes de cancelación de suscripción inmediatamente.

- Si envía correo electrónico que contiene enlaces, verifíquelos con la lista de bloqueo de dominios (DBL) de Spamhaus. Para probar sus enlaces, utilice la herramienta de búsqueda de dominios en el sitio web de Spamhaus.

Al implementar estas prácticas, puede mejorar su reputación de remitente y aumentar así la probabilidad de que el correo electrónico que envía alcance las bandejas de correo de los destinatarios. La implementación de estas prácticas también ayuda a mantener baja la tasa de rebotes y de reclamaciones de su cuenta, y reduce el riesgo de enviar correo electrónico a trampas de spam.

Preguntas frecuentes sobre métricas de envío de correo electrónico de Amazon SES

Amazon SES recopila varias métricas acerca de los mensajes de correo electrónico que envía. Estas métricas le permiten analizar la eficacia de su programa de correo electrónico y monitorizar estadísticas importantes como, por ejemplo, las tasas de rebotes y reclamaciones.

En esta sección, se incluyen preguntas frecuentes relacionadas con los siguientes temas relacionados con las métricas de envío de correo electrónico:

- Preguntas generales
- Seguimiento de aperturas
- Seguimiento de clics

> **Note**
>
> El seguimiento de eventos depende del proveedor de servicios de correo electrónico (ESP) del destinatario y de cómo ha configurado su configuración de privacidad, lo cual está fuera del control de Amazon SES. El recuento de eventos de seguimiento se puede sesgar (devolver recuentos inexactos) en condiciones como las siguientes:
>
> - El destinatario del correo electrónico utiliza un proveedor de servicios de correo electrónico (ESP) que protege su privacidad.
> - El destinatario del correo electrónico no da permiso explícitamente a su ESP para compartir sus datos.

- El ESP del destinatario del correo electrónico almacena en caché imágenes o enlaces, SES solo puede contar la apertura inicial, pero no podrá contar las aperturas posteriores.

Preguntas generales

Q1 (P1). Una vez que se entrega un correo electrónico, ¿durante cuánto tiempo sigue Amazon SES recopilando métricas de aperturas y clics?

Amazon SES recopila métricas de aperturas y clics durante 60 días después de que se envíe cada correo electrónico.

Q2 (P2). Si un usuario abre un correo electrónico varias veces o hace clic en un enlace de correo electrónico varias veces, ¿se realiza un seguimiento de cada uno de estos eventos por separado?

Si un destinatario abre un correo electrónico varias veces, Amazon SES cuenta cada apertura como un evento de apertura único. Del mismo modo, si un destinatario hace clic en el mismo enlace varias veces, Amazon SES cuenta cada clic como un evento de clic único. Sin embargo, estos recuentos se pueden sesgar según los escenarios descritos anteriormente en el cuadro de notas.

Q3 (P3). ¿Las métricas de apertura y clic están agregadas o se pueden medir hasta el nivel de destinatario?

El seguimiento de aperturas y clics se realiza en el nivel de destinatario. Gracias al seguimiento de aperturas y clic, puede determinar qué destinatarios han abierto un correo electrónico o han hecho clic en un enlace del correo electrónico.

P4. ¿Puedo recuperar métricas de aperturas y clics utilizando la API de Amazon SES?

La API de Amazon SES no proporciona ningún método para recuperar las métricas de aperturas y clics. Sin embargo, puede recuperar las métricas de aperturas y clics para Amazon SES utilizando la API de CloudWatch. Por ejemplo, puede utilizar la AWS CLI para recuperar las métricas de clics mediante la API de CloudWatch emitiendo el siguiente comando:

```
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
```

El comando mostrado más arriba recupera el número total de eventos de clic para cada día en 2017. La recuperación de las métricas de apertura cambia el valor del parámetro `metric-name` a `Open`. También puede modificar los parámetros `start-time` y `end-time` para cambiar el periodo de análisis o cambiar el parámetro `period` para análisis más detallado.

Seguimiento de aperturas

Q1 (P1). ¿Cómo funciona el seguimiento de aperturas?

Una imagen GIF transparente de 1 píxel por 1 píxel se inserta en cada correo electrónico enviado a través de Amazon SES e incluye una referencia única a este archivo de imagen; cuando la imagen se descarga, SES puede decir exactamente qué mensaje se abrió y quién lo hizo.

De forma predeterminada, este píxel se inserta en la parte inferior del correo electrónico; sin embargo, algunas aplicaciones de proveedores de correo electrónico truncan la vista previa de un correo electrónico cuando supera un determinado tamaño y pueden proporcionar un enlace para ver el resto del mensaje. En este escenario, la imagen de seguimiento de píxeles de SES no se carga y eliminará las tasas de apertura que intenta rastrear. Para evitar esto, puede colocar de forma opcional el píxel al principio del correo electrónico o en cualquier otro lugar mediante la inserción del marcador de posición `{{ses:openTracker}}` en el cuerpo del correo electrónico. Una vez que SES recibe el mensaje con el marcador de posición, se sustituirá por una imagen de píxel de seguimiento abierta.

> **Important**
>
> Simplemente agregue un marcador de posición `{{ses:openTracker}}`, ya que más de uno provocará que se devuelva un código de error `400 BadRequestException`.

La incorporación de este píxel de seguimiento no cambia el aspecto de su correo electrónico.

P2. ¿El seguimiento de aperturas está habilitado de forma predeterminada?

El seguimiento de aperturas está disponible para todos los usuarios de Amazon SES de forma predeterminada. Para utilizar el seguimiento de aperturas, debe hacer lo siguiente:

1. Cree un conjunto de configuración.
2. En el conjunto de configuración, cree un destino de eventos.

3. Configure el destino de eventos para publicar notificaciones de eventos de apertura en un destino.
4. En cada correo electrónico en el que desea realizar el seguimiento de aperturas, especifique el conjunto de configuración que ha creado en el paso 1.

Para obtener más información sobre cómo habilitar el seguimiento abierto a través de un destino de eventos de un conjunto de configuración, consulte the section called “Crear destinos de eventos”. Puede utilizar el marcador de posición de píxeles en Correo electrónico SMTP de estas maneras: formateado, sin procesar y correo electrónico con plantilla.

Obtenga más información sobre cómo Supervisar el envío de correo electrónico mediante la publicación de eventos.

Q3 (P3). ¿Puedo omitir el píxel de seguimiento de apertura en determinados correos electrónicos?

Hay dos formas de omitir el píxel de seguimiento de apertura en sus mensajes de correo electrónico. El primer método consiste en enviar el correo electrónico sin especificar un conjunto de configuración. De forma alternativa, puede especificar un conjunto de configuración que no esté configurado para publicar los datos sobre eventos de apertura.

P4. ¿Se realiza el seguimiento de apertura en correos electrónicos de texto sin formato?

El seguimiento de apertura solo funciona con correos electrónicos en HTML. Dado que el seguimiento de apertura se basa en la inclusión de una imagen, no es posible recopilar métricas de apertura de los usuarios que abren los correos electrónicos a través de un cliente de correo electrónico de solo texto (no HTML).

Seguimiento de clics

Q1 (P1). ¿Cómo funciona el seguimiento de clics?

Para realizar un seguimiento de clics, Amazon SES modifica cada enlace en el cuerpo del correo electrónico. Cuando los destinatarios abren un enlace, se los envía a un servidor de Amazon SES e inmediatamente se los reenvía a la dirección de destino. Al igual que con el seguimiento de apertura, cada enlace de redireccionamiento es único. Esto permite a Amazon SES determinar qué destinatario hace clic en el enlace, cuándo hace clic y el correo electrónico desde el que se ha llegado al enlace.

> **Important**
>
> Si envía un único mensaje a varios destinatarios, cada destinatario guardará el mismo enlace de seguimiento de clic. Para realizar un seguimiento de la actividad de clic de los destinatarios individuales, envíe correo electrónico a un destinatario por operación de envío.

Q2 (P2). ¿Puedo deshabilitar el seguimiento de clics?

Puede deshabilitar el seguimiento de clics añadiendo un atributo, `ses:no-track`, a las etiquetas delimitadoras en el cuerpo HTML de su correo electrónico. Por ejemplo, si enlaza a la página de inicio de AWS, un enlace delimitador normal se asemejaría a lo siguiente:

```
<a href="https://aws.amazon.com">Amazon Web Services</a>
```

Para deshabilitar el seguimiento de clics en ese enlace, modifíquelo para que se parezca a lo siguiente:

```
<a ses:no-track href="aws.amazon.com">Amazon Web Services</a>
```

Dado que `ses:no-track` no es un atributo HTML estándar, Amazon SES lo elimina automáticamente de la versión del mensaje de correo electrónico que llega a las bandejas de entrada de sus destinatarios.

También puede deshabilitar el seguimiento de clics en todos los mensajes que envíe mediante un conjunto de configuración específico. Para deshabilitar el seguimiento de clics, modifique el destino de eventos del conjunto de configuración para que no registre eventos de clic.

Para obtener más información sobre cómo habilitar y desactivar el seguimiento de clics a través del destino de eventos de un conjunto de configuración, consulte the section called “Crear destinos de eventos”.

Obtenga más información sobre cómo Supervisar el envío de correo electrónico mediante la publicación de eventos.

Q3 (P3). ¿Cuántos enlaces se pueden rastrear en cada correo electrónico?

El sistema de seguimiento de clics puede rastrear un máximo de 250 enlaces.

P4. ¿Se recopilan métricas de clics en enlaces de correos electrónicos de texto sin formato?

Solo es posible realizar un seguimiento de los clics en correos electrónicos HTML.

P5. ¿Puedo etiquetar enlaces con identificadores únicos?

Puede añadir un número ilimitado de etiquetas, como pares de clave-valor, a enlaces en su correo electrónico utilizando el atributo `ses:tags`. Al utilizar este atributo, especifique las claves y los valores utilizando el mismo formato que utilizaría para transferir propiedades CSS en línea: escriba la clave, seguida de dos puntos (:), seguida del valor. Si necesita transferir varios pares de clave-valor, separe cada par con un punto y coma (;).

Por ejemplo, imagine que desea añadir las etiquetas `product:book, genre:fiction, subgenre:scifi, type:newrelease` a un enlace. El enlace resultante se asemeja a lo siguiente:

```
<a ses:tags="product:book;genre:fiction;subgenre:scifi;type:newrelease;"
    href="http://www.amazon.com/…/">New Releases in Science Fiction</a>
```

Estas etiquetas se transmitan a través de su destino de publicación de eventos, por lo que puede llevar a cabo un análisis adicional en los enlaces específicos en los que los usuarios han hecho clic.

> **Note**
>
> Las etiquetas de enlace pueden incluir los números del 0 al 9, las letras de la A a la Z (mayúsculas y minúsculas), guiones (-) y guiones bajos (_).

P6. ¿Los enlaces de seguimiento utilizan el protocolo HTTP o HTTPS?

Los enlaces de seguimiento utilizan el mismo protocolo que los enlaces originales en su correo electrónico.

Por ejemplo, si su correo electrónico incluye un enlace a `https://www.amazon.com`, el enlace es reemplazado por un enlace de seguimiento que utiliza el protocolo HTTPS. Si su correo electrónico incluye un enlace a `http://www.example.com`, el enlace es reemplazado por un enlace de seguimiento que utiliza HTTP. Si su correo electrónico incluye ambos enlaces mencionados

anteriormente, el enlace HTTPS se reemplaza por un enlace de seguimiento que utiliza el protocolo HTTPS y el enlace HTTP se reemplaza por un enlace de seguimiento que utiliza el protocolo HTTP.

P7. Hay un enlace en mi correo electrónico del que no se está realizando un seguimiento. ¿Por qué no?

Amazon SES espera que los enlaces de los correos electrónicos contengan direcciones URL codificadas correctamente. En concreto, las direcciones URL de los enlaces deben cumplir la norma RFC 3986. Si un enlace de un correo electrónico no está codificado correctamente, los destinatarios podrán ver el enlace, pero Amazon SES no realizará un seguimiento de los eventos de clic para dicho enlace.

Normalmente, los problemas relacionados con una codificación incorrecta ocurren en las URL que contienen cadenas de consulta. Por ejemplo, si la URL de un enlace del correo electrónico contiene un carácter de espacio no codificado en la cadena de consulta (como el espacio entre “John” y “Doe” en el siguiente ejemplo: http://www.example.com/path/to/page?name=John Doe), Amazon SES no realizará un seguimiento de ese enlace. Sin embargo, si la URL utiliza un carácter de espacio codificado en su lugar (como “%20” en el siguiente ejemplo: http://www.example.com/path/to/page?name=John%20Doe), Amazon SES hará un seguimiento del enlace según lo previsto.

Índice de búsqueda rápida

El siguiente índice se ha creado para ayudarle a encontrar rápidamente cosas en Amazon SES, proporcionando dos formas de búsqueda: por instrucciones o por conceptos. Los instrucciones describen cómo hacer algo, mientras que los conceptos explican el panorama general.

Denos su opinión

Utilice el botón Feedback (Comentarios) que se encuentra en la esquina superior derecha para informarnos...

- ¿Le ha resultado útil este índice?
- ¿Hay algunas instrucciones o conceptos que le gustaría ver agregados a este índice?
- ¿Hubo algo que pensó que debería haber sido categorizado de manera diferente?

Enlaces a instrucciones y conceptos de SES

How-tos

Los enlaces de procedimientos de SES se enumeran alfabéticamente y lo llevarán a la sección correspondiente para mostrarle “cómo” realizar la acción que seleccionó.

- Aprenda cómo…
  - Agregue un registro SPF como parte de la configuración de un dominio MAIL FROM personalizado
  - Asignar grupos de IP
  - Bloquear el SPAM para la recepción de correo electrónico
  - Configurar dominios de aperturas y clics personalizados
  - Configurar notificaciones de SNS
  - Conectarse a un punto de conexión de SMTP
  - Crear un conjunto de configuración
  - Crear una identidad de dominio
  - Crear una identidad de dirección de correo electrónico
  - Crear destinos de eventos

- Crear filtros de direcciones IP
- Crear un grupo de IP administradas para habilitar IP dedicadas (administradas)
- Crear una regla de recepción
- Crear alarmas de reputación con CloudWatch
- Crear una política de autorización de envío mediante una política personalizada
- Crear una política de autorización de envío utilizando el generador de políticas
- Crear grupos de IP dedicadas estándar para direcciones IP dedicadas (estándar)
- Eliminar una identidad
- Eliminar datos personales
- Editar una identidad
- Habilitar el reenvío de retroalimentación de correo electrónico
- Exportar métricas de reputación
- Salir del entorno aislado
- Introducción a SES
- Introducción a Virtual Deliverability Manager
- Conceder permisos para recibir correos electrónicos
- Aumentar el rendimiento
- Aumentar las cuotas de envío
- Integración de con su servidor de correo electrónico existente
- Registrar llamadas a la API
- Administrar conjuntos de configuración
- Administración de Easy DKIM y BYODKIM
- Supervisar métricas de envío y reputación
- Supervisar las estadísticas de envío
- Supervisar las estadísticas de uso
- Supervisar su cuota de envío
- Obtener registros de DKIM para una identidad
- Obtener las credenciales de SMTP
- Anular la supresión de nivel de conjunto con supresión del nivel establecido de configuración
- Anular la firma DKIM heredada en una identidad de dirección de correo electrónico

- Pausar el envío de correo electrónico
- Publicar un registro MX
- Informar del uso abusivo de los recursos de AWS
- Solicitar direcciones IP dedicadas
- Solicitar asistencia técnica
- Resolver problemas de capacidad de entrega y reputación con el asesor de Virtual Deliverability Manager
- Recuperar datos de eventos desde CloudWatch
- Recuperar datos de eventos desde Kinesis Data Firehose
- Recuperar datos de eventos de desde SNS
- Enviar un correo electrónico mediante un SDK de AWS
- Enviar correo electrónico mediante programación
- Enviar correo electrónico usando API de SES
- Enviar correo electrónico mediante SMTP
- Enviar un correo electrónico sin procesar con un archivo adjunto mediante la CLI o la API de SES
- Enviar correos electrónicos de prueba mediante el simulador de buzones
- Configurar BYODKIM: utilice su propio DKIM
- Configurar una política DMARC
- Configuración de Easy DKIM
- Configurar la recepción de correos electrónicos
- Configurar la publicación de eventos
- Configurar un dominio MAIL FROM
- Configurar autorización de envío (tareas de propietario de identidad)
- Configurar autorización de envío (tareas de remitente delegado)
- Especificar un conjunto de configuración al enviar correo electrónico
- Probar la conexión a la interfaz de SMTP
- Tasas de rebotes y reclamaciones
- Comprender las propiedades de firma DKIM heredadas
- Usar las métricas de reputación
- Usar los paquetes de software para el envío de correo electrónico

- Usar la administración de suscripciones
- Usar plantillas para el envío de correo electrónico
- Usar su lista de supresión a nivel de cuenta
- Verificar una identidad de dominio
- Verificar una identidad de dirección de correo electrónico
- Ver una identidad
- Consultar vistas generales y detalladas de las métricas de capacidad de entrega de la cuenta mediante el panel Virtual Deliverability Manager
- Ver métricas de SNDS para direcciones IP dedicadas
- Preparar direcciones IP dedicadas

Concepts

Los enlaces a conceptos de SES se enumeran alfabéticamente y lo llevarán al capítulo y las secciones correspondientes para explicar el concepto que seleccionó.

- Encuentre información sobre...
  - Uso abusivo de los recursos de AWS, informe
  - Panel de cuenta
  - Lista de supresión a nivel de cuenta
  - Opciones de acción para recibir correos electrónicos
  - Agregar acción de encabezado
  - Tipos de adjuntos no admitidos
  - Acción de devolución de respuesta de rebote
  - BYODKIM: utilice su propio DKIM
  - BYOIP (Traiga su propia IP)
  - Ejemplos de código
  - Validación de conformidad
  - Supresión de nivel de conjunto de configuración
  - Conjuntos de configuración
  - Codificaciones de contenido
  - Soporte heredado de notificaciones entre cuentas

- Dominios MAIL FROM personalizados
- Protección de los datos
- Direcciones IP dedicadas
- Direcciones IP dedicadas (administradas)
- Direcciones IP dedicadas (estándar)
- Autenticación de correo electrónico con DKIM
- DMARC (Autenticación, informe y conformidad del mensaje basado en el dominio)
- Conformidad con DMARC a través de DKIM
- Conformidad con DMARC a través de SPF
- DKIM fácil:
- Destino de reenvío de retroalimentación de correo electrónico
- Authentication acerca de la recepción de correo electrónico
- Conceptos de recepción de correo electrónico
- Explicaciones de la consola acerca de la recepción de correo electrónico
- Análisis de malware en el correo electrónico entrante
- Permisos de recepción de correo electrónico
- Casos de uso de recepción de correo electrónico
- Restricciones de recepción de correo electrónico
- Métodos de autenticación del envío de correo electrónico
- Puntos de conexión
- Notificaciones de eventos
- Notificaciones a través de correo electrónico
- Notificaciones a través de SNS
- Publicación de eventos
- Preguntas frecuentes
- Lista de supresión global
- Campos de encabezado admitidos
- Administración de identidades
- Administración de identidades y accesos

- Seguridad de infraestructuras

- Acción de integración con Amazon WorkMail
- Control basado en IP mediante filtros de dirección IP
- Acción de invocación de una función de Lambda
- Administración de listas
- Listas y suscripciones
- Registro y monitoreo
- Detección de malware
- Firma DKIM manual
- Supervisar el envío de correo electrónico mediante la publicación de eventos
- Supervisar reputación del remitente
- Monitoreo de la actividad de envío
- Cuotas
- Reglas de recepción
- Control basado en destinatarios mediante reglas de recepción
- Regiones
- Métricas de reputación
- Mensajes de métricas de reputación
- Resiliencia
- Entregar a la acción del bucket de S3
- Entorno aislado: salir de
- Seguridad
- Protocolos de seguridad compatibles
- Autorización de envío
- Anatomía de la política de autorización de envío
- Ejemplos de políticas de autorización de envío
- Proceso de autorización de envío
- Métricas de SNDS para direcciones IP dedicadas
- Contenidos de notificación de SNS
- Ejemplos de notificación de SNS

- Acción de publicación en un tema de SNS

- SPF: marco de políticas de remitente
- Acción de detención del conjunto de reglas
- Administración de suscripciones
- Asistencia, solicitar de tipo técnico
- Plantillas para la verificación de correo electrónico personalizada
- Solución de problemas
- Identidades verificadas
- Virtual Deliverability Manager
- Puntos de conexión de la VPC

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.